CCNA

Introduction

[1] Network definition

[2] network components:-
* HTTP * FTP * SMTP * pop3 * Telnet

[4] Network topologies
* p-p * star * BUS * mesh * ring

[5] Network types
* LAN * WAN * MAN

[8] OSI Model

[12] TCP/IP Model

[13] Typical Network Components
* pc * Hub * switch * Router * Modem

[15] DTE & DCE

[16] physical layer
* LAN cables

[18] LAN standards & Twisted pair Categories

[19] LAN connectors
* Straight & cross & consol cables

[23] Data link layer
* MAC address
* types of dst MAC { unicast, Broadcast, multicast }

[25] MAC Method
* CSMA/CD

[26] MAC Flow control
* Buffering * congestion avoidance
MAC Frame

[28] layer 2 devices
* NIC * Bridge * switch

[29] Switch operation
* learning

[30] Forwarding
* Flood If Nst MAC { unknown unicast, multicast, Broadcast }

[31] Microsegmentation
* to avoid collision in switch

[32] switch Forwarding Modes (types)
* cut through * Fragment Free
* store & forward * adaptive cut through

[33] Remove L2 loops (STP)

[34] L3: internet layer

[35] Router operation
* learning * forwarding

[36] IP V4
* TOS * TTL

[37] ICMP (internet control Messaging protocol)
→ * ping www.facebook.com
→ * Trace wwi.facebook.com

[38] IPV4 classes
- Class A, B, C, D, E
- Classless IPs

[41] NAT

[42] Subnetting

[45] Getting started for end to end data delivery
-src IP Manually

[46] - automatically [DHCP]

[47] . dst ip

[48] dst MAC [ARP] address resolution protocol

[50] L4: transport layer
- Port no & socket no

[51] TCP & UDP in L4

[53] OLD subnetting standard

Routing

[54] Routing introduction
- Routed & Routing protocol
- static & dynamic Routing

[55] Autonomous sys.

[56] admis. distance - metric

[57] Static routing → ~~y~~ !

[58] Distance vector [RIPv1]

[59] at start up

[60] at convergance, at change

[62] Triggered update +poison rout & reverse

[63] split horizon

64 Hold down timer

65 RIPv1 & IGRP C/C's

66 Advanced D.V
* Rip V2

67 EIGRP
* Start up

69 at convergance

70 at change

72 EIGRP C/C's

73 Link State
* ospf * Start up

75 - at change
- at convergence
- ospf c/c's

76 Hirarchical design

78 Route summarization
and CIDR
(Super networking)

80 ospf operation in multiple access
* Router ID

81 neighor discovery

82 Routes discovery
* Electing of DR & BDR

83 VLSM [Variable Length Subnet Mask]

84 NAT
* static * dynamic

85 PAT

switching

86 STP (at start up)
* BPDU flooding * Electing root switch and root port

89 Electing Disignated port
* Blocked port

91 at change
* direct & indirect change

92 RSTP

94 VLAN
* inter VLAN Routing

1 Traditional solution
2 Router on a stick
3 multilayer switch

96 switch port types
* access * Trunk

97 Tagged types
* ISL * IEEE 802.1q

98 VLAN Configuration

99 static & Dynamic VLAN membership

100 DTP

100 Managing switch remotely

101 VTP
* VTP operation

104 wi Fi

105 wifi Standards
IEEE 802.11 b/G/n/A

106 wifi design
* ad hoc * infrastructure mode

108 WAN switching
108 * circuit switching
109 * packet ~
110 * Broadband Technology

111 DSL
* ADSL * SDSL

111 C.S protocols
* encapsulation
* HDLC * PPP
* configuration

113 PPP operation
* LCP * NCP

114 PPP Negotiation
- error correction - Compression
- multilink - Call Back
- Authentication

115 PAP - CHAP authentic

116 CSU/DSU Digital Modem

117 Packet switching (FR)
- FR Encapsulation

118 FR operation
- LMI - IARP

120 FR issue & solutions

122 Security
- types of attacks

125 Switch security

126 Router ~
- ACL types

127 IP Standard ACL
- create ACL

128 - activate ACL & Examples

130 Ip Extended ACL
- Create ACL

131 activate ACL & EX

132 firewall

134 IDS & IPS

135 VPN

136 - VPN devices & protocols
- VPN operation ⇄ C I A

139 security types
- PSK - WPA - WPA 2

140 IPV6

143 NDP

144 IPV6 types (addressing)

145 APIPA

146 IPV6 end to end data delivery
* MPLS * MobileIP

147 IPV4 to IPV6 translation
* Dual Stack * NAT-PT
* Tunneling

149 How to recover password

Network definition / it is a group of components that are connected together to provide a service ← application

Mobile Network
Telephony ~] → they are not our course

⇒ our course is about data network (IP Network)

Network Importance

① Easy sharing of files, information and data
② Easy sharing of Expinsive resources (devices)
③ Modern live
- voice over IP
- vedio conference
- Telepresense
- smell
- touch
- Games (as call of duty)
- life

Network components

[1] Computer / it is the main component, because it is the soure of Network application
↳ services that can be done with a remote device

operating systems
- windows
- Linux
- Unix
- Mac OS
- android ⟶ OS for Mobile
- ios ⟶ OS for apple devices

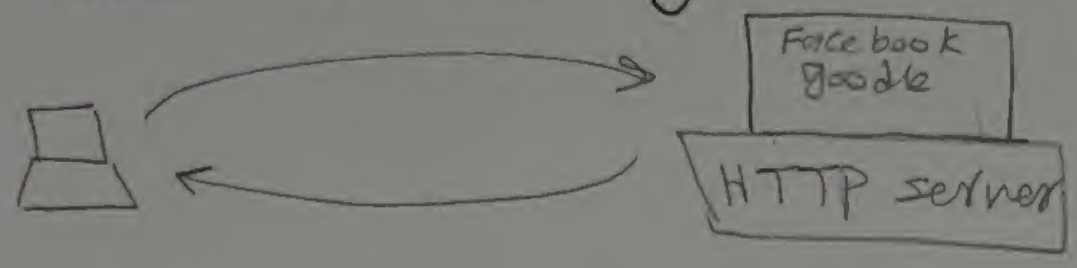
Examples of Network applications

protocol is set of rules

EX1 HTTP (Hyper text transfere protocol)

Hyper text as [Text, pic, audio, vedio]

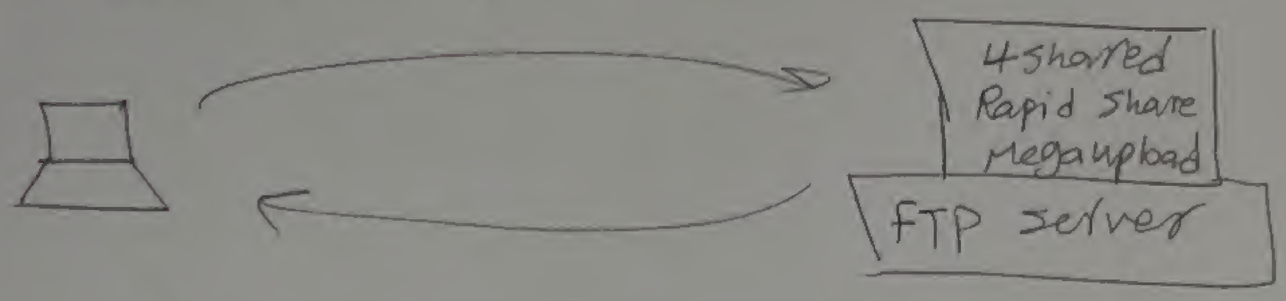
* it is used for browsing



EX 2 FTP (File transfere protocol)

Huge files

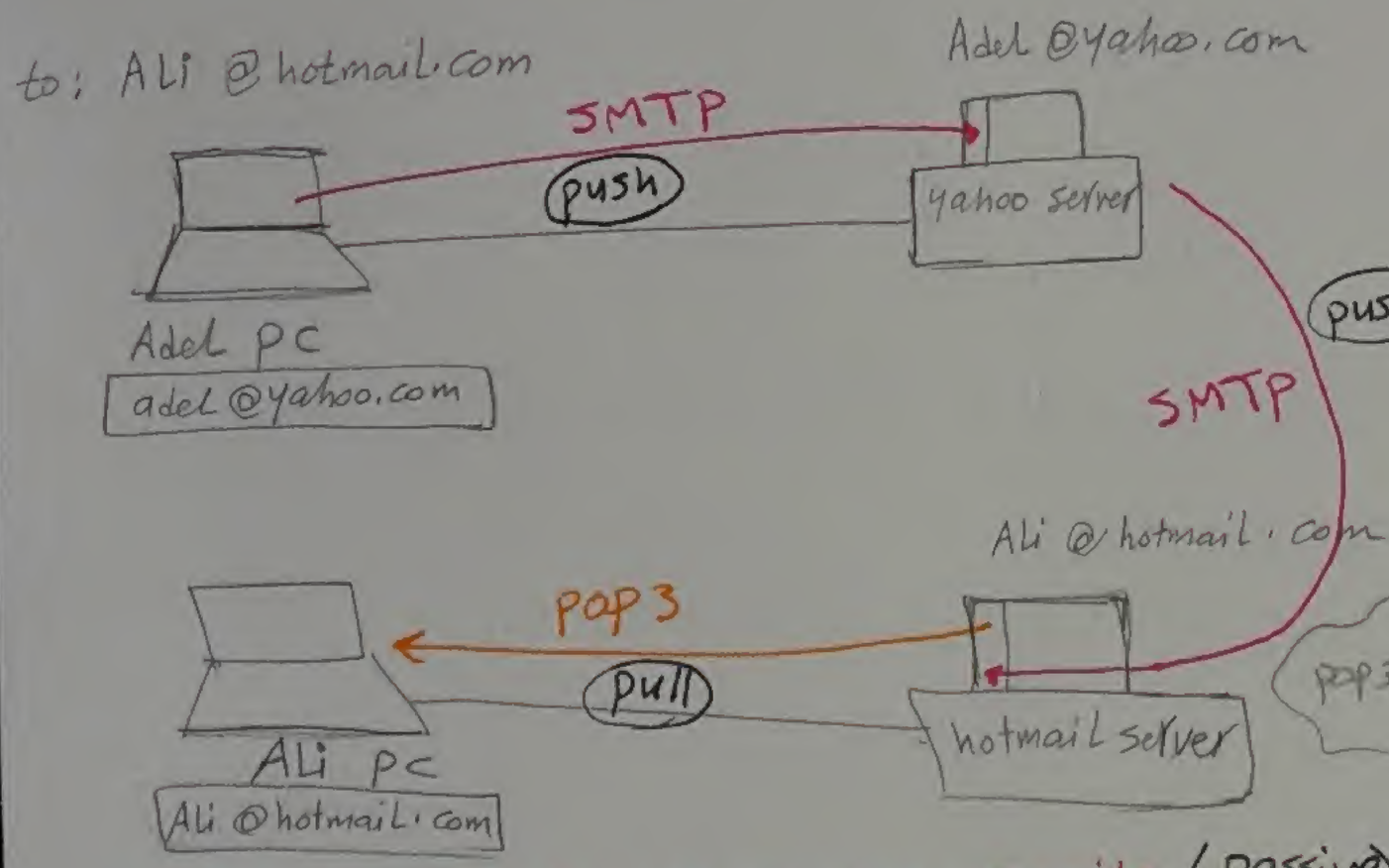
* it is used for upload and download data



EX 3 Telnet

* It is used for remote login

EX 4 - SMTP (simple Mail transfere protocol)
- pop 3 (post office protocol version 3) } used for using electronic mails



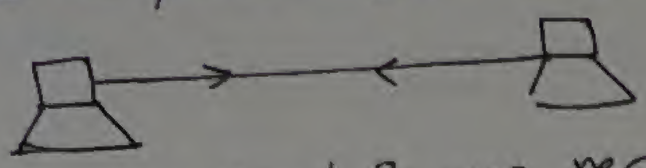
distination & source انا عشان
ومن حالتين
① لو ال dst. بيـ Receive
ال Mail ، يبقى بيعمل العمليه دى
ال SMTP

② لو ال dst. بيسحب (retreive)
ال Mail ، يبقى بيعمل العمليه دى ال pop3

SmTp is used for receiving Emails (passive)
pop3 is used for retrieving Emails (active)

Network Topologies :-

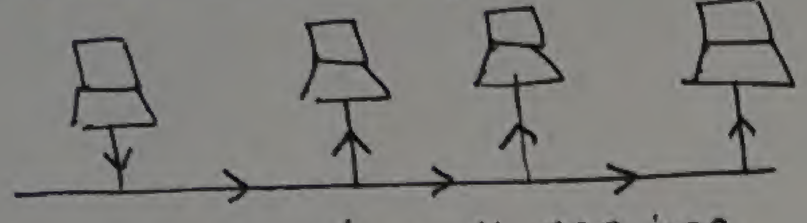
[1] point to point topology



one send & one receive

---

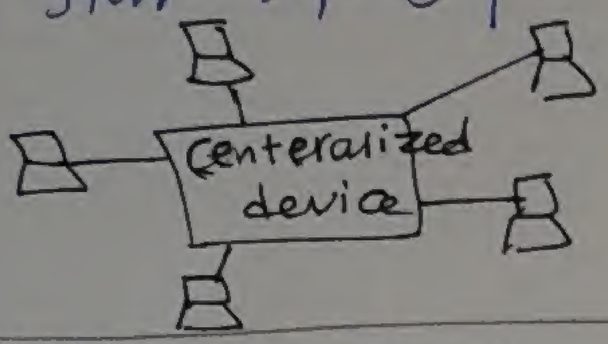
[2] Bus topology



one send , all receive

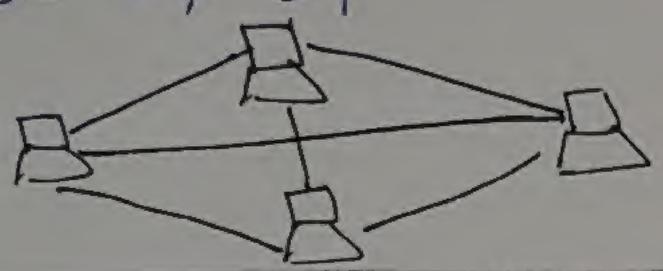
---

[3] Star topology



---

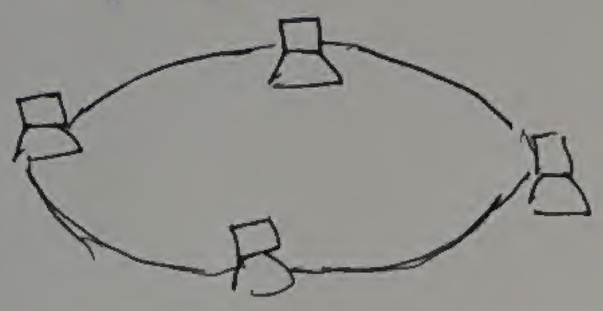
[4] Mesh topology



no of connections = $\frac{n(n-1)}{2}$

---

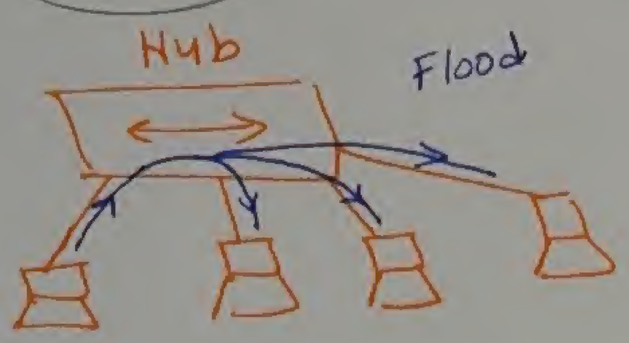
[5] Ring topology



---

physical topology v.s logical topology

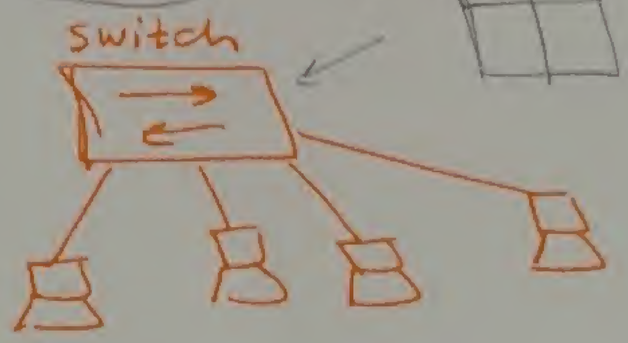
EX.1



physical : star

logical : Bus

EX.2

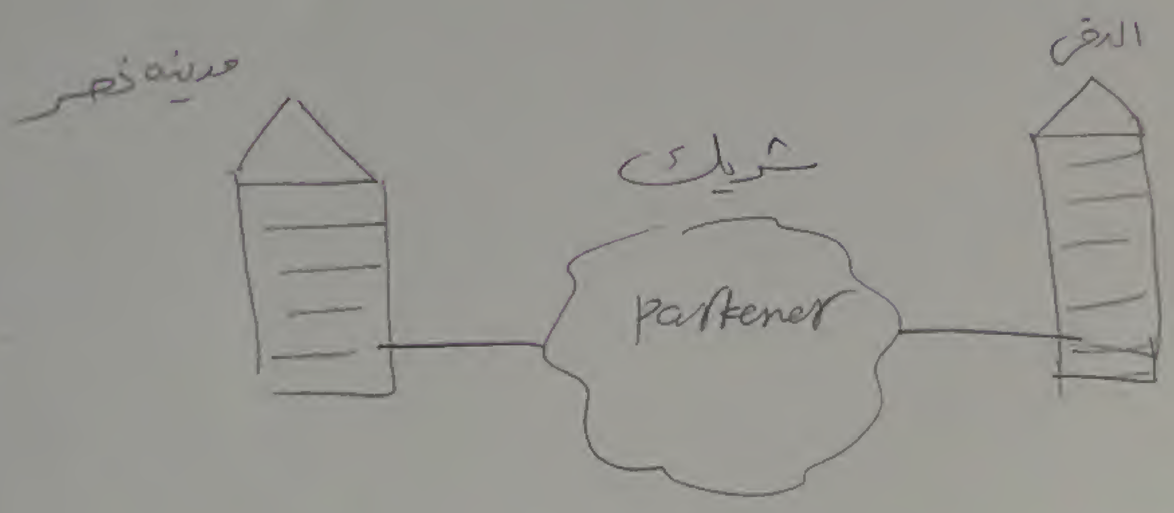


physical : star

logical : Mesh

Network types

LAN : local Area network	MAN : Metropolitan area Network	WAN : wide area network
it is a group of Components connected one operator to gether in a small area	⇒ it is a group of LANs withen the same city	⇒ it is Group of LANs between cities & contries & continents
EX : Ethernet → 10 Mbps Fast Ethernet → 100 Mbps GiGa Ethernet → 1 G bps 10 GiGa ~ → 10 Gbps		⇒ Internet is the biggest WAN EX : X.25 ATM Frame relay



In case of partener, the LAN is converted to WAN

If there is no partenar, it is still LAN

Network is

group of component ---> connected together ---> to provide aservice

* end devices
- computer , IP phone , IP T.V , IP cam , play station

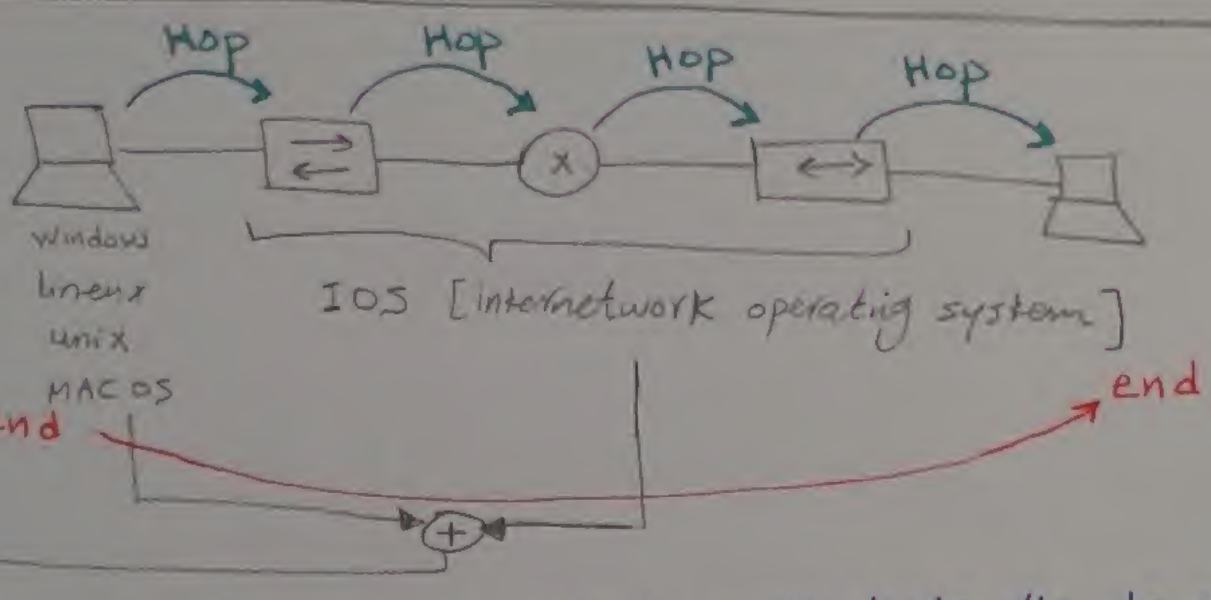
* Intermedite devices
- Hub , Router, switch

* connectivity

Topology
- point to point
- BUS
- star
- Mesh
- Ring

- data
- voice
- life
- vedio

LAN , MAN , WAN



Network model / it is all concepts that will help the devices to know How to send data hop to hop and then end to end

Network model is some layer :-

* What is a layer? / it is a function that can be done either by S/W or H/W
* why layer ? / because functions are sequential

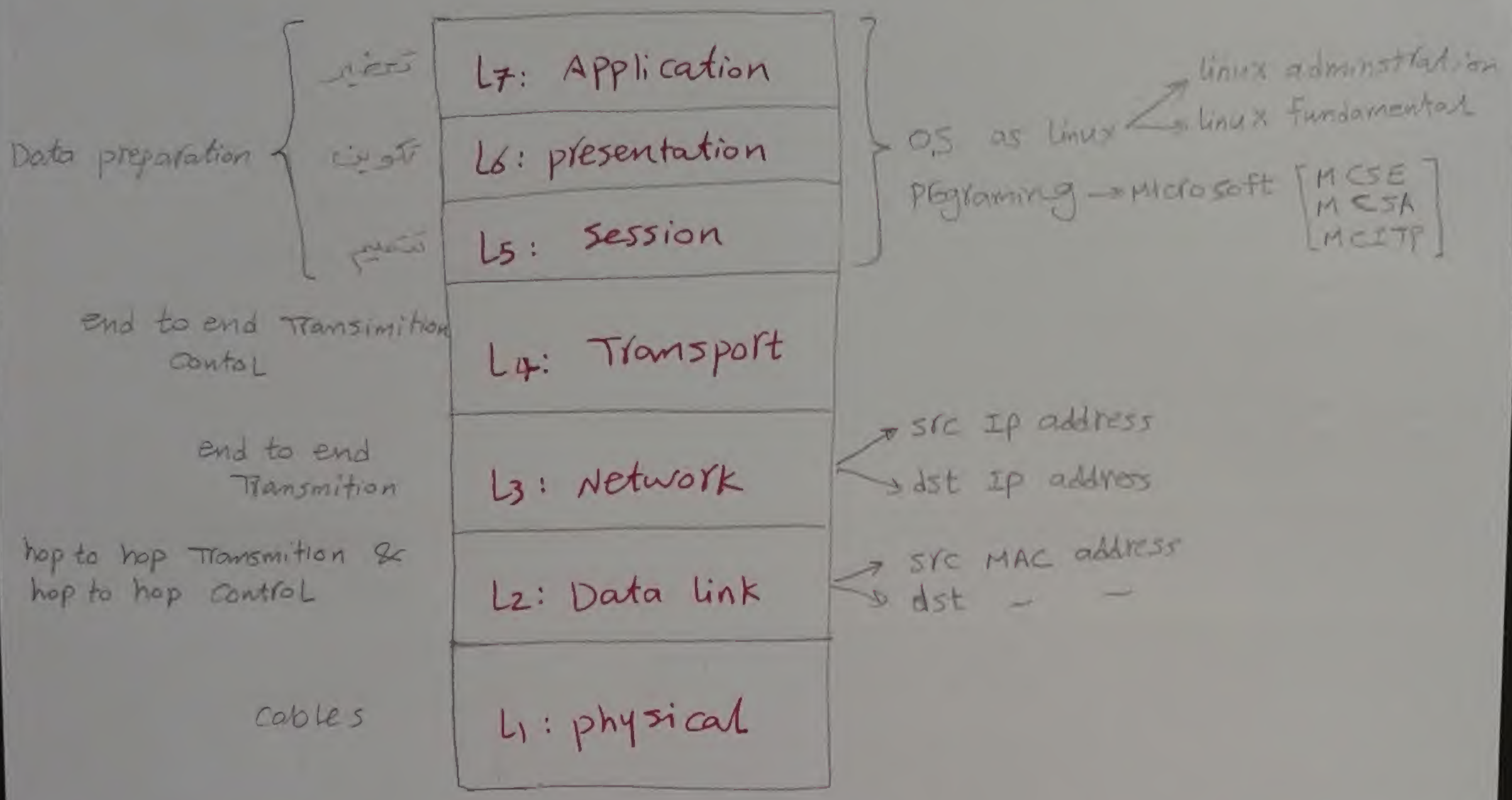
example of Network Models :-
open standard
open sourse

① OSI Model [open system interconnection] developed by ISO and it is used as reference model

② Tcp/Ip [DOD model] Department of Defence,
↳ commertial model ⇒ developed by DARPA وزارة الدفاع الامريكية

→ it is closed model
حتى مسموح لحد يطور فيه

OSI Model



L7 : Application layer : it is responsible for Making the proper data preparation For the proper service

ex: service → application

Browsing → HTTP

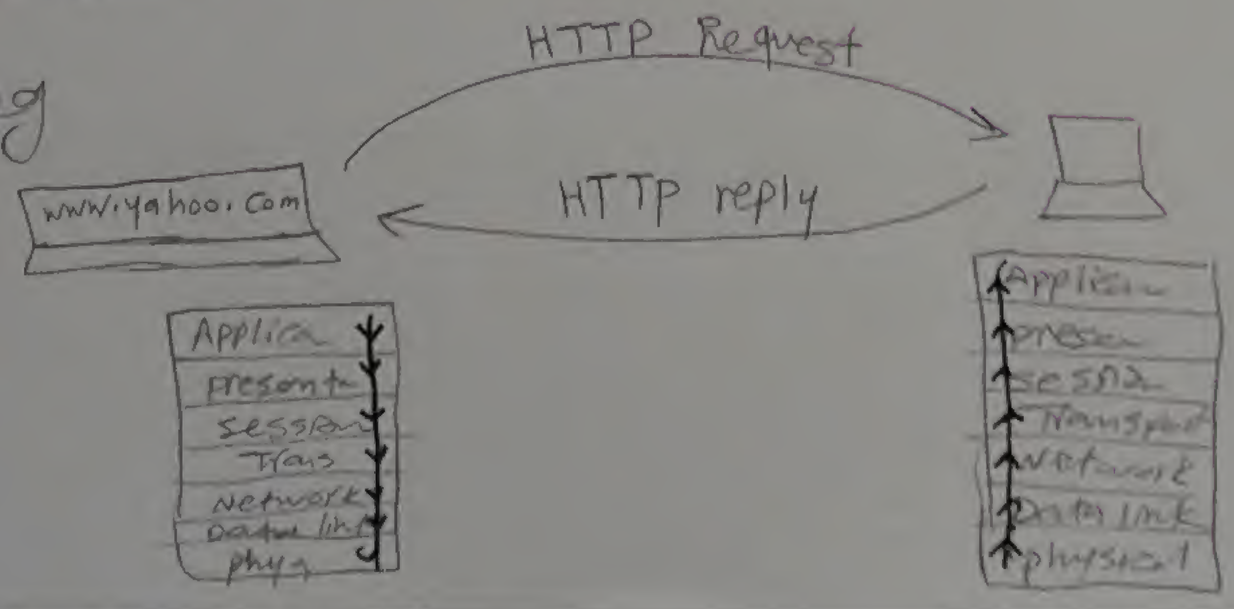
File upload & download → FTP

send / retrieve mail → SMTP / POP3

remote login → Telnet

Video, voice, games → RTP [real time Tranfere protocol]

EX on Browsing



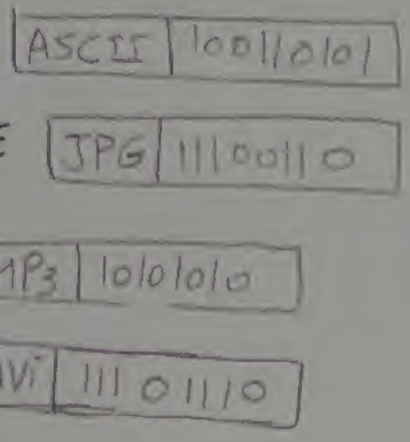
L6 : representation layer : it is responsible for finding common data representation between src & dst

Text → ascII

PIC → JPG , GIE

audio → Midi , MP3

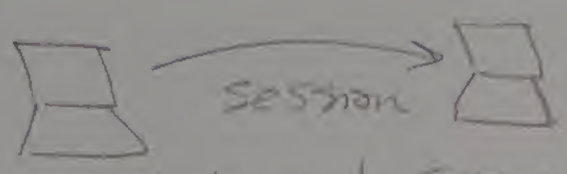
video → AVi , M pay



L5 : session layer : it is responsible for making sure that all information required for session opening become ready & in that case it will give orders for

العقل المدبر

1 - session establishment
2 - session Management
3 - session Termination



end to end communication

يشابه بناءً كبير انه كل تاجه صح قبل ما يكمل Communiat

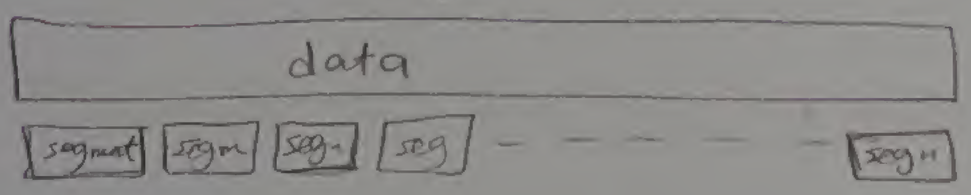
L4 : Transport layer : it is responsible for the actual Mechanism of : ينفذ الاوامر

الجلسات

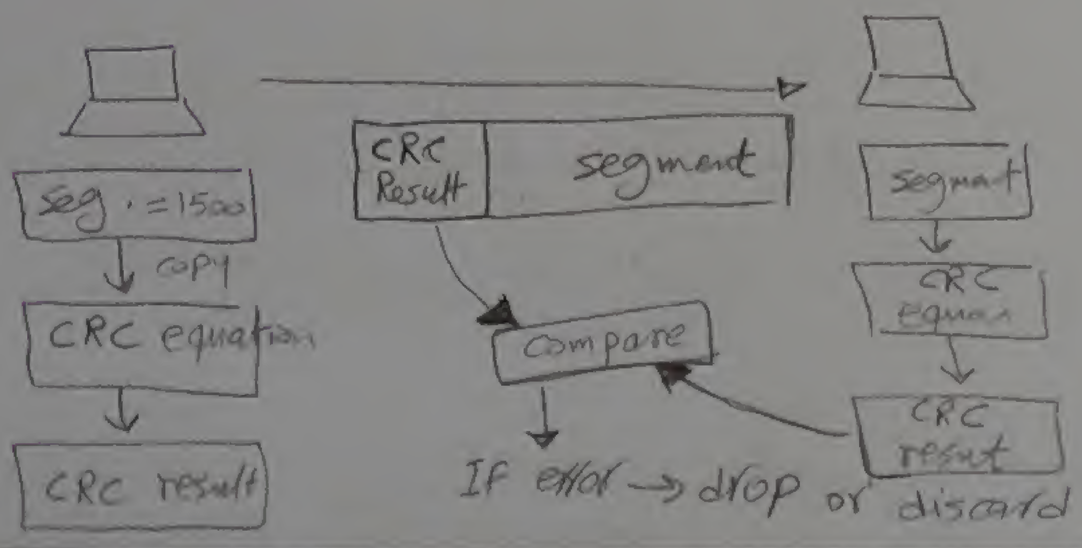
1 - session establishment
2 - session Termination
3 - session management

Transport layer function :-

[1] segmentation :- Deviding data into smaller segments

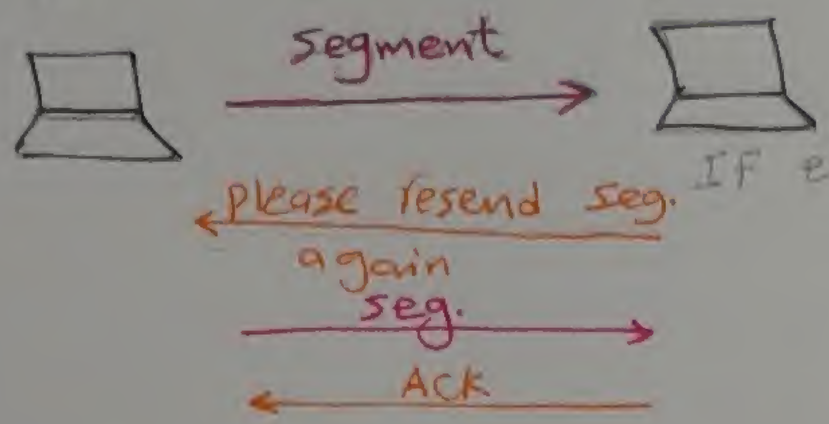


[2] error Detection :- by CRC [cyclic redundancy check] = 4 byte



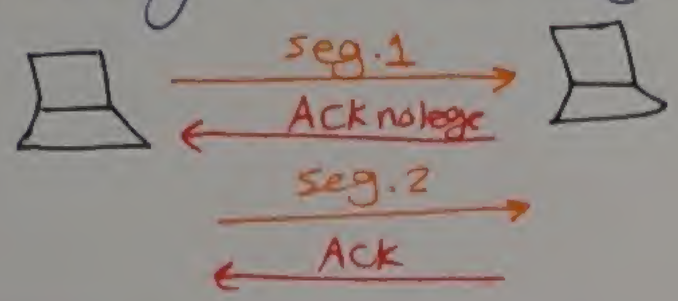
[3] segmentation sequancing :- giving serial no to each segment

[4] error collection :-



---

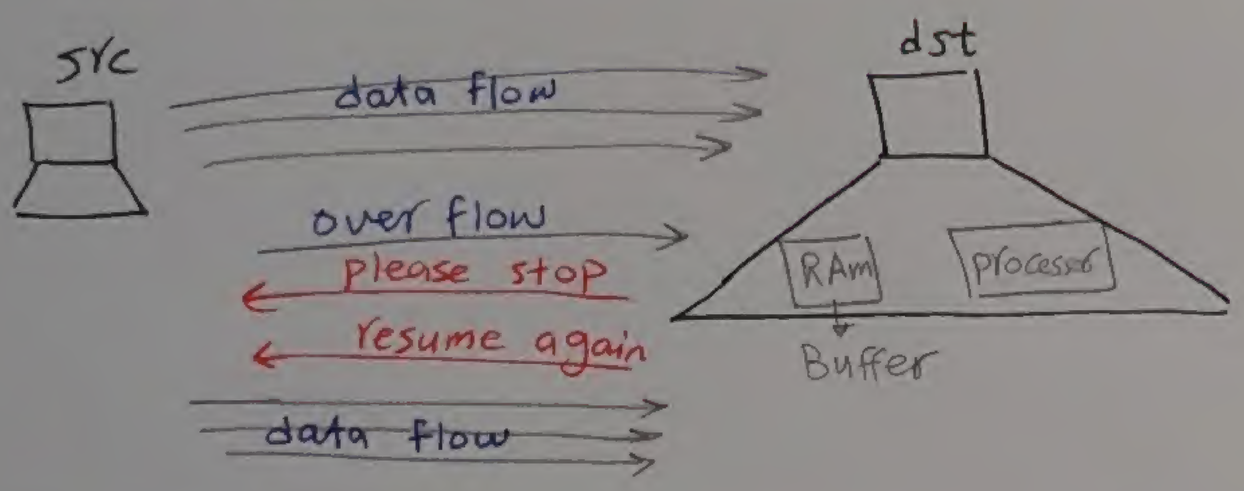
[5] Reliability :- Making sure that segments are correctly received



(Ack) بمعنى الرد بـ

---

[6] flow control



في حالة ان الـ RAm امتلت او الـ processor اشتغل جداً ← الـ dst هيبعت رساله الى src ويقوله stop please وبالشكله resume again تحمل هيقوله

---

types of s/w that is founded in Transport layer and excute all these steps above

[1] TCP : Transmittion control protocol [يهتم بالدقة]
excute 100% of Transport layer functions [the 6 above]
used in HTTP, FTP, SMTP, POP3

[2] UDP : user datagrame protocol [يهتم بالانجاز]
excute 25% of Transport layer functions
used in RTP

L3 : Network layer : it is responsible for end to end data delivery

ex. of protocols Founded in L3 : IPv4, IP V6, IPx, Apple TAIK

it is responsible for → src IP address
dst IP address

Ip address is an address used to identify end devices
[used as final end address]

L2: Data link layer / it is responsible for hop to hop data delivery and control

it is responsible for physical addressing and switching (finding the best path for next hop)

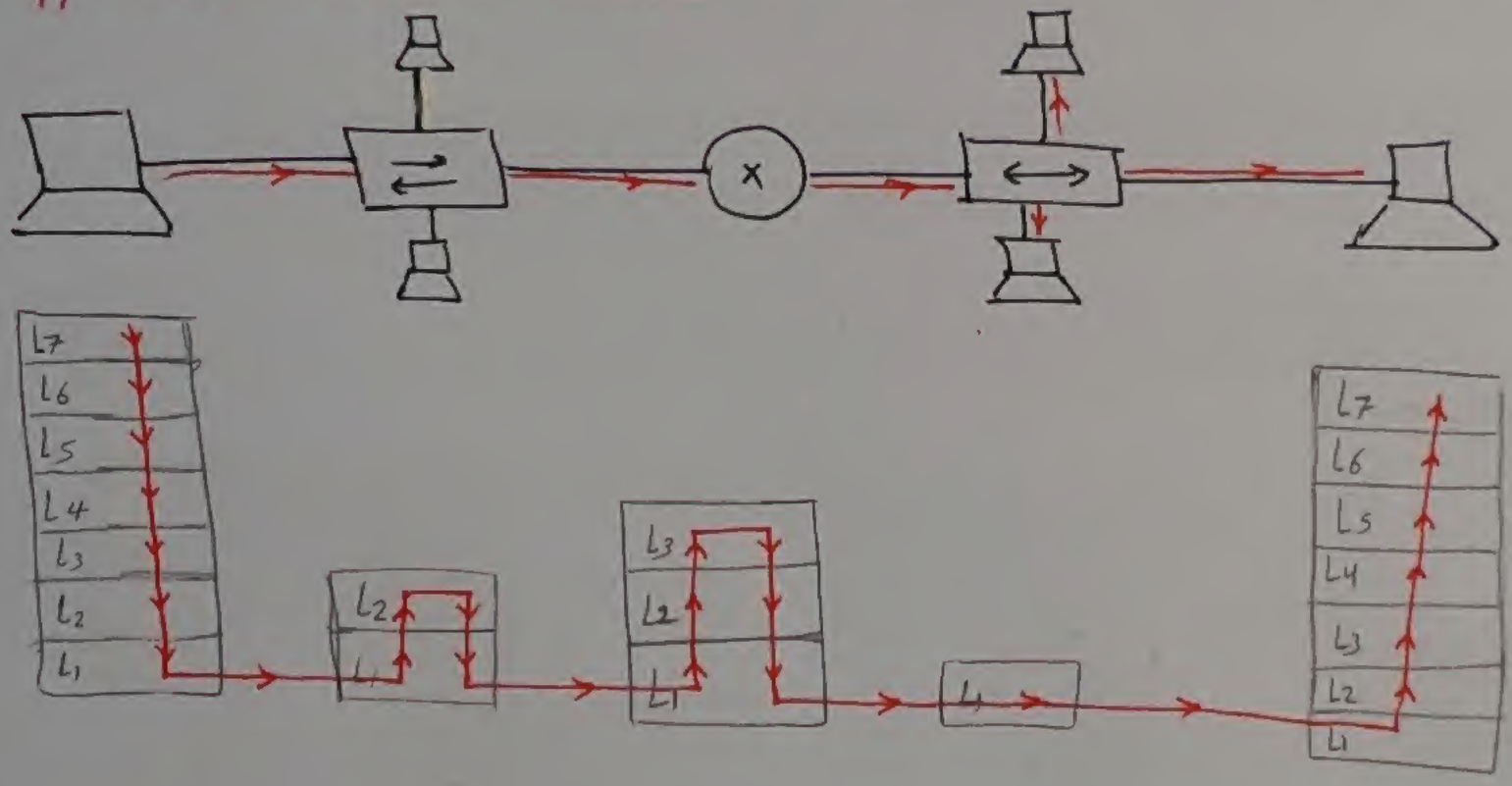
ex. of protocols Founded in Data link layer (L2)

LAN
- Ethernet
- wi fi

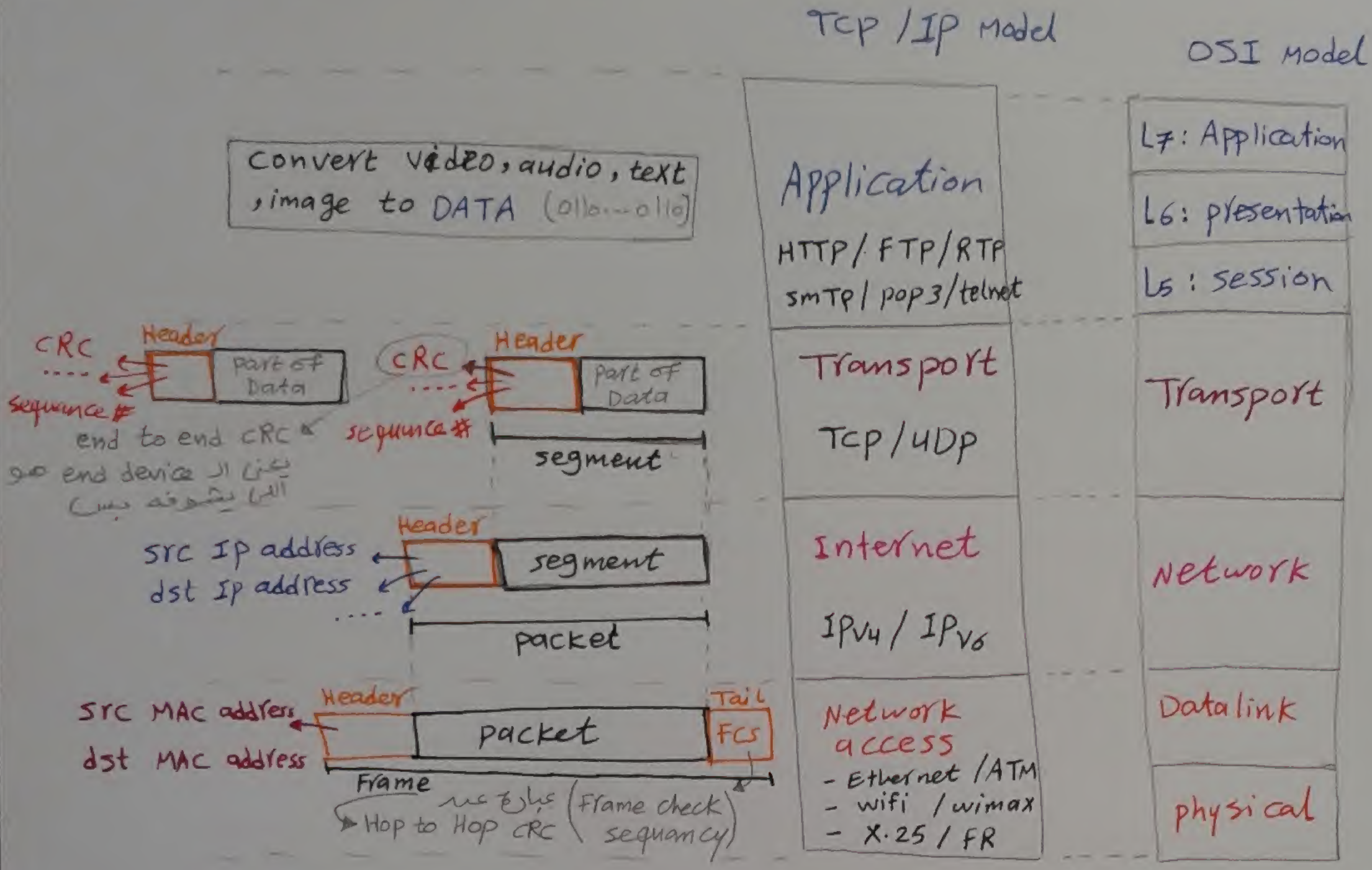
WAN
- Frame relay
- X.25
- ATM
- DSL
- wimax

---

* Typical Network Model



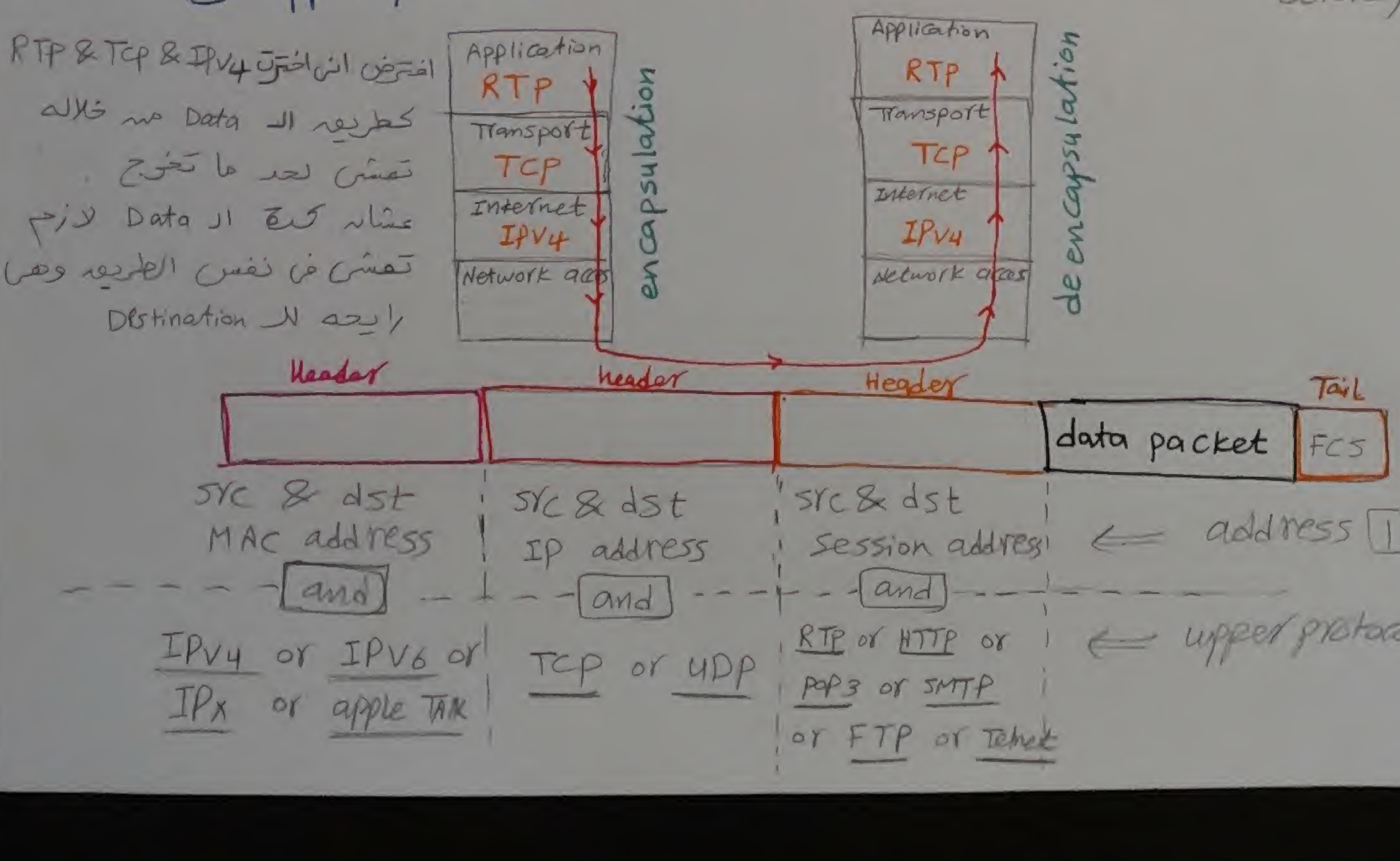
Note 1: layer 2 devices can by default understand layer 1
Note 2: when Data is drop , the device that wants it is the one who request for it



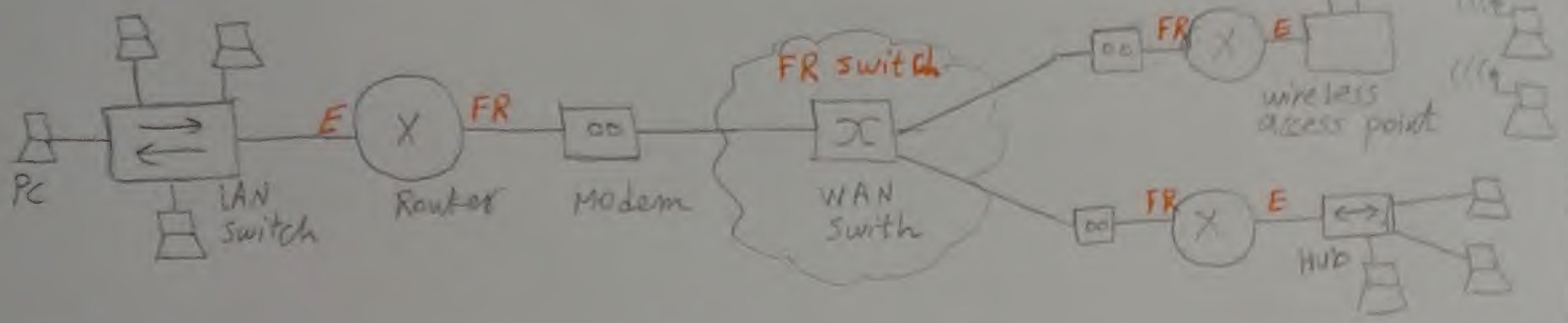
---

* Each layer adds a header to a data part, each header contains :-

1. address
2. upper protocol (pointer to upper protocol that is allready used before)



* Typical network components

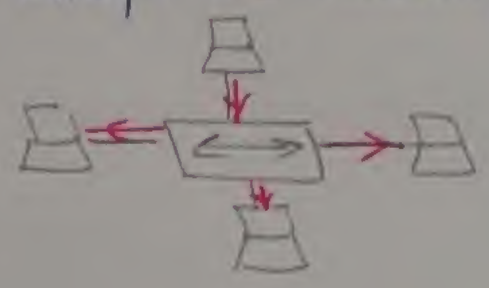


[1] Computer [end device]

* it is a soura of application
* it is L7 devica
* the proper physical topology is → Star topology

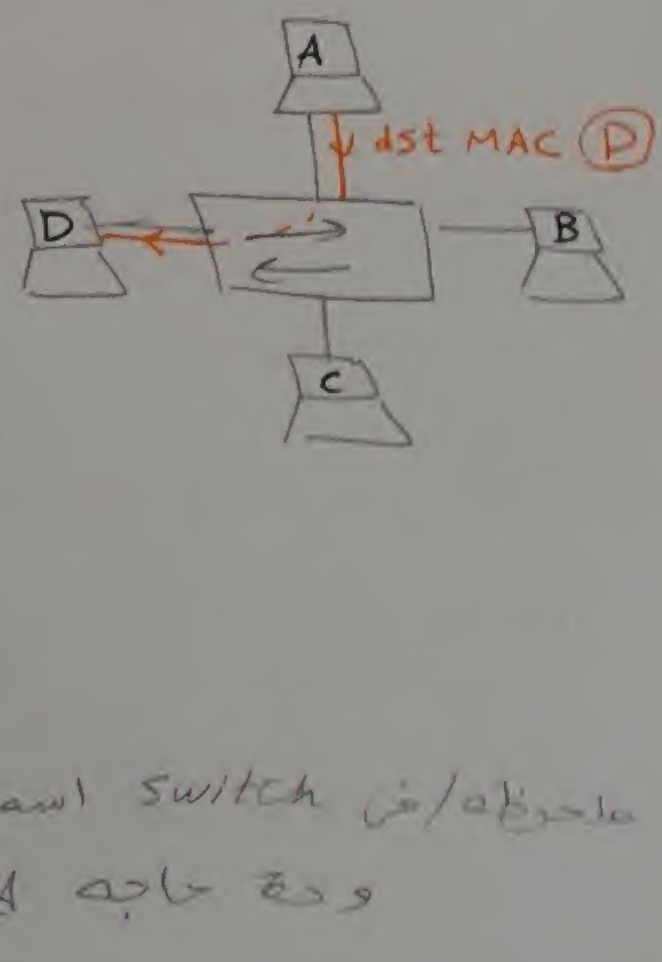
[2] Hub ⟺

* it is centeralized devica used to produce physical star topology
* it doesn't know neither Final address(Ip address)nore next hop(MAC address)
* it Floods data / defining data out of all ports except the receiving port
* it is transparent devica (not a hop)



[3] switch ⇄

* it is a centoralized devica, used to provide a physical star topology
* it doesn't know how to reach Final end (IP address) but it knows how to reach next hop (MAC address)
* it is layer 2
* it is transperent devica (not a hop)



هو ملهوش MAC عشان كدة كدة ال Data لازم تعدي عليه ولكنه عندة جداول يقدر منه خلالها يحدد ال Data رايحه فين (next hop) من خلال ال MAC اللى موجود فى ال packet

ملحوظة/ ال switch اسمه (Multi layer switch) دة يقدر يفهم لحد layer 7 وده حاجه advanced هتعرفها فى الكورس

* all its ports of switch should use only single communi. Technology

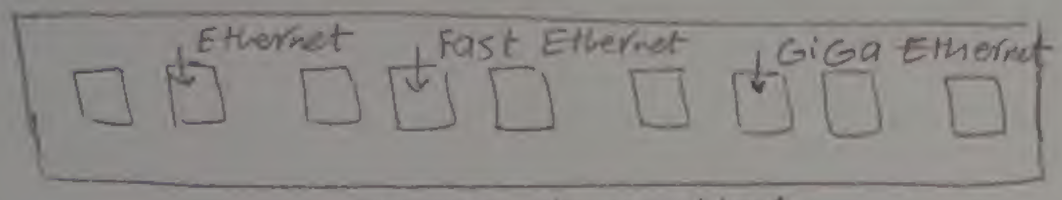
يعني انه كل الـ ports في الـ switch الواحد مسموحه مستقبل التكنولوجيا

communication Technology

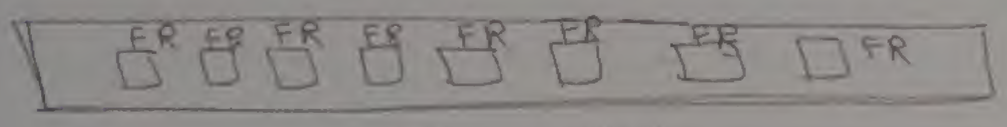
LAN comm. Tech.
- Ethernet
- wifi

WAN comm. Tech.
- X.25
- FR
- ATM
- ISDN
- DSL
- wimax

ex

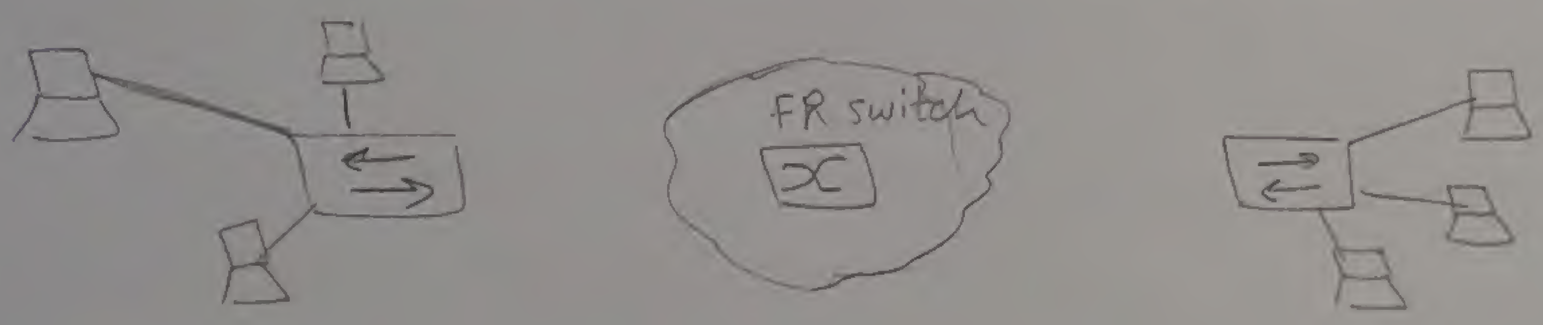


Ethernet switch



FR switch

المشكله هنا ان الـ Ethernet لـ max distance = 100m مبيقدرش استخدمه لمسافات طويله ، طيب لو رحت لـ FR switch (WAN switch) ده هيحل مشكله المسافات لكنه الكروت الـ Network غاليه اوى و خليك فاكر ان كل الـ ports في الـ switch الواحد ليها نفس Communication Technology



عشان المشكله دى ← اما استخدم كل 100m (switch Ethernet) او ادفع كتير اوى واستخدم (WAN switch) عشان الـ fiber و ثمن الكارت اصلا غالى اوى

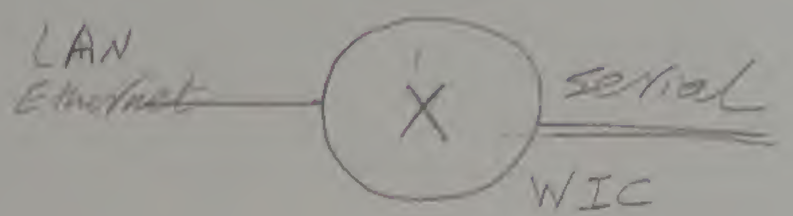
لازم اذهب الى الـ Router

LAN switch	WAN switch
- high data rate - cheap - lower range distance	- low data rates - very Expensive - higher range distance

4) wireless switch
* it is air switch
* it is layer 2

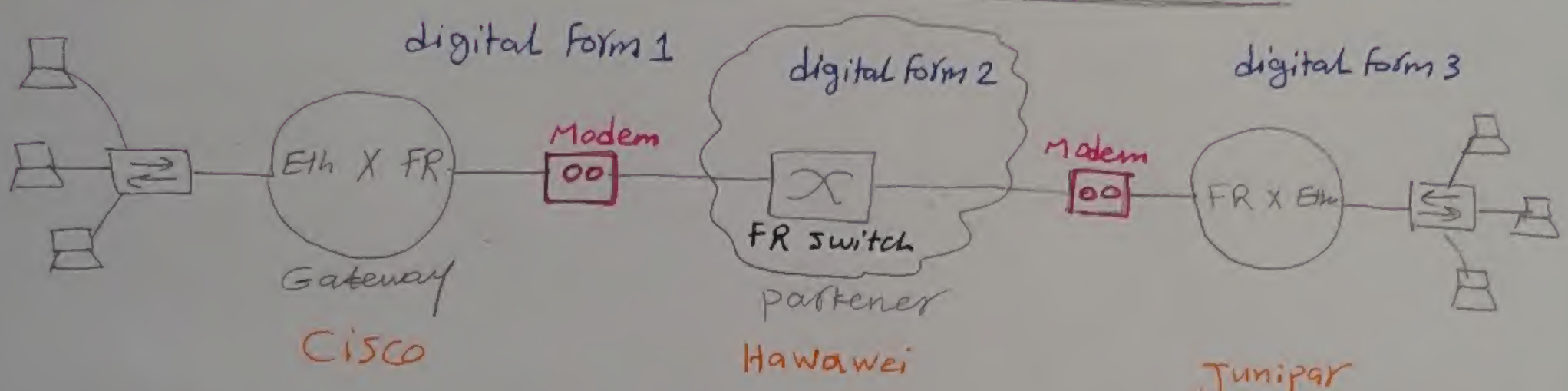
5 Router

* it is a device that support multiple technologies by S/W
* it has interfaces LAN Technologies and WAN Technologies
* it can understand Ip address and MAC address
* the disadvantage of Router that it has more delay and very Expensive

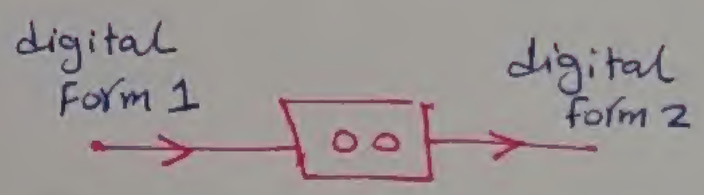


WIC : WAN Interface Card

- X.25
- FR
- ATM
- !



6 modem [modulator - demodulator]



It is used for :-

1- change digital forms ≡ line coding → to satisfy serveca provider
2- support clocking & syncronization

note/ there isn't moden in LAN because in LAN, there is autoclocking in Ethernet that match clocking automatically

* it is layer 1 devica

devices are classified in to

1 DTE [Data terminal Equip.]

* it is adevice that can be either src or dst For data and information
* it should be at least layer 3

ex : PC & Router

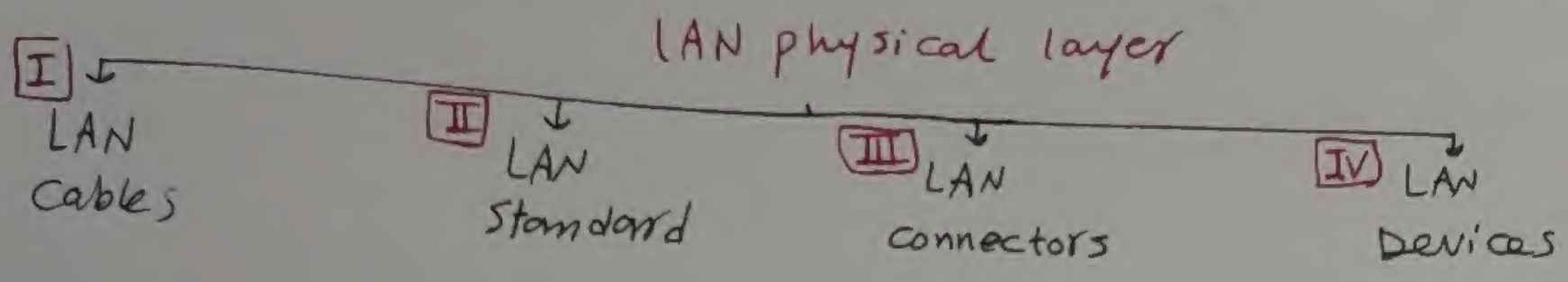
2 DCE [Date communication Equipment]

* it is adevica that can be either a centeralized devica or suppor clocking and syncromization
* it is at most layer 2

ex : Hub, switch, Modem, wireless access point

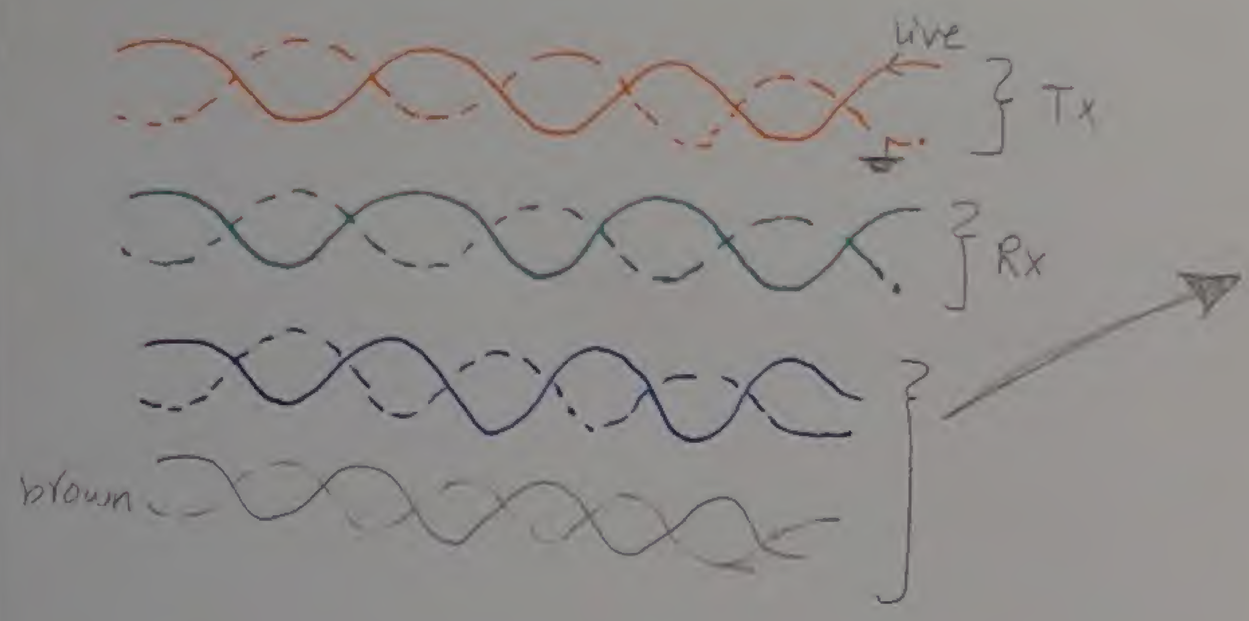
* physical layer [LAN الـ layer الأول في الـ OSI model]

PDU [protocol Data unit] = Bits



I LAN Cables

a. UTP : unshilded twisted pair [8 wires e.g 4 pairs]



* بيستخدم الـ brown & blue
Very High Data rate الـ all-
GiGa & 10 GiGa Ethernet في
and POE [power over Ethernet]

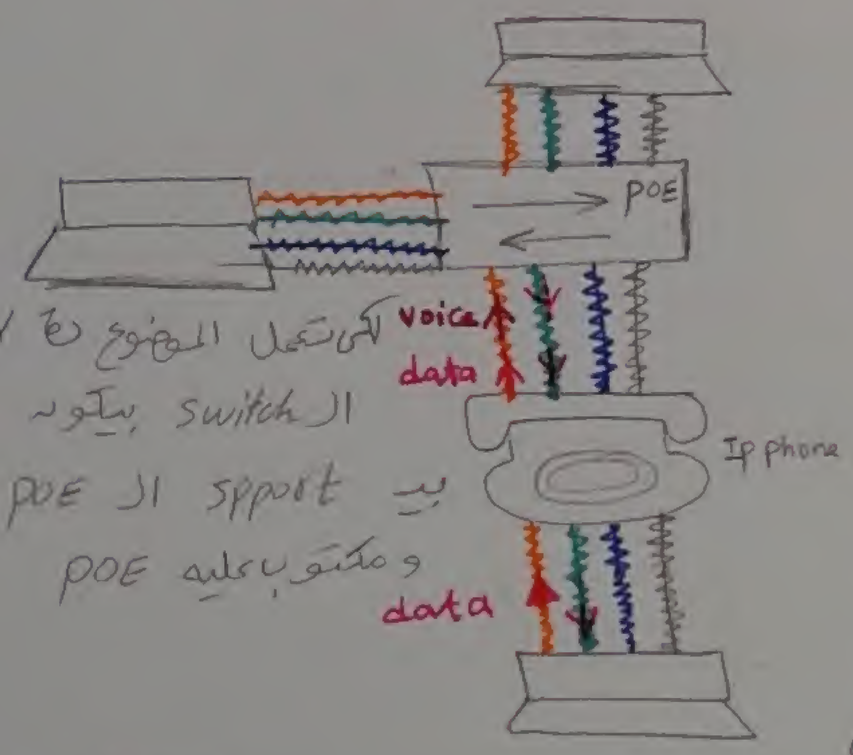
* الـ Ip phone ليه IP و MAC

* الـ Voice بياخد 64 kbps

لو الكابل بيشيل 100Mbps

64 kbps for voice — The rest for data

* الـ Voice دايماً بيسبق الـ data



لكي تشغل الموضوع ده لازم
الـ switch بيكون
بيـ support الـ POE
و مكتوب عليه POE

* لو انت بتبعت بـ data rate
زي الـ Giga 6 كده انا بستخدم
الـ 4pairs و بالتالي الـ Ip phone
Vcc = 5 ← 3pair
GRN = 0 ←
Vcc = 53 ← 1 pair
GRN = 48 ←

* the case of twisting
1- prevent electromagnitic interference and radio interference
2- prevent (cross talk) ← تداخل
(e.g) cancle the existance of capacitance by inductance

Ip phone لـ power وبيجي الـ

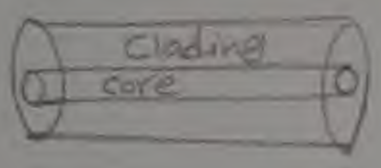
[b] STP : sheilded Twisted pair

it is used to protect the signal from External low voltage difference

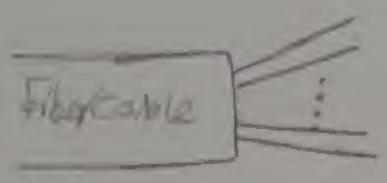
but If There is a high voltage difference, I have to use a Fiber

note/ both UTP & STP are used when maximum distance = 100 m

[c] Fiber



high light = 1
low light = 0



advantage of fiber ① Immunite against electric noise
② very high speed
③ support long distance
but it is very expinsive

Fiber

MMf (Multimode fiber)
core diameter = 62.5 Mm, 50 Mm
cladding diameter = 125 Mm
400 m ⟶ 4 km

SMf (single mode fiber)
core diameter = 9 Mm, 8 Mm
cladding diameter = 125 Mm
10 km ⟶ 100 km

* each device wants one pair of fiber wires, one for Tx & one for Rx

note/ In LAN Network we don't use fiber because it is very expinsive
but we can use Ethernet that support speeds up to 10 GHz

II LAN Standards

IEEE 802.3 ⟶ standard for Ethernet

1980 — February

Ethernet standard types :-

- 10 Base T
- 100 Base T — Twisted pair whose maximum distance = 100 m
- 1000 Base T

← Fiber

- 10 Base F
- 100 Base F
- 1000 Base SX — short distance → less 4 km [use MMF]
- 1000 Base LX — long distance → 10 km [use MMF]
- 1000 Base ZX — extra long distance → 100 km [use SMF]

speed in Mbps

Base band ≡ no need for modulation

Interview question

what type of Ethernet that you should use ?? Choose 2 answers

sol :-

① 1000 Base LX → the best because it is cheaper and do the same work

② 1000 Base ZX

* twisted pair cable categories

Cat 5 → 100 Mbps

Cat 5e → 1 Gbps

Cat 6 (enhanced) → up to 4 Gbps

] 100m

Cat 6A → 10 Gbps] 25 m

Cat 6E (advanced) → 10 Gbps

Cat 7 → up to 40 Gbps

] 100 m

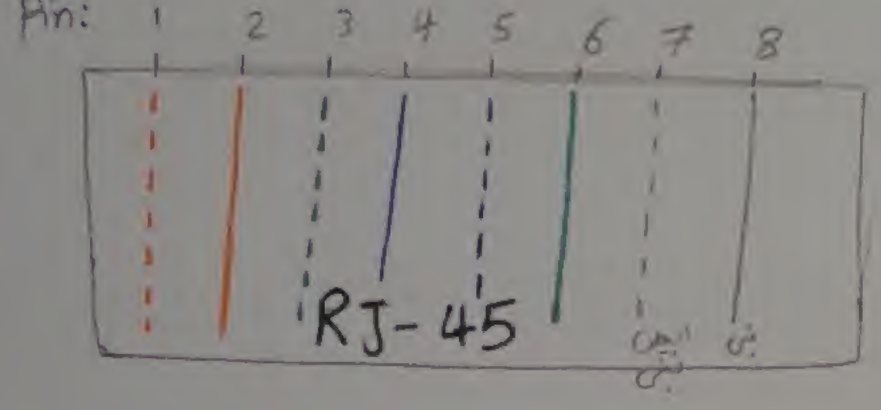
III LAN connectors

Fiber connectors

* ST : straight Tip
* SC : square connector

Copper connectors

* DB ≠ D-shaped [ex: DB-21 , DB-60]
* RJ : Register jack [ex: RJ11 , RJ45]



ملحوظة / الـ Data بتعدي الالوان الفاتحه وبتستخدم
لـ Rx & Tx ⇐ الالوان الفاتحه هي Orange & Green

IP	Standard B	Standard A
	Pin 1,2 → Orange	Pin 1,2 → Green
	Pin 3,6 → Green	Pin 3,6 → Orange
	This standard is called T568B (Standard B)	This is a standard called T568A (Standard A)

* Connection types :-

LAN DTE

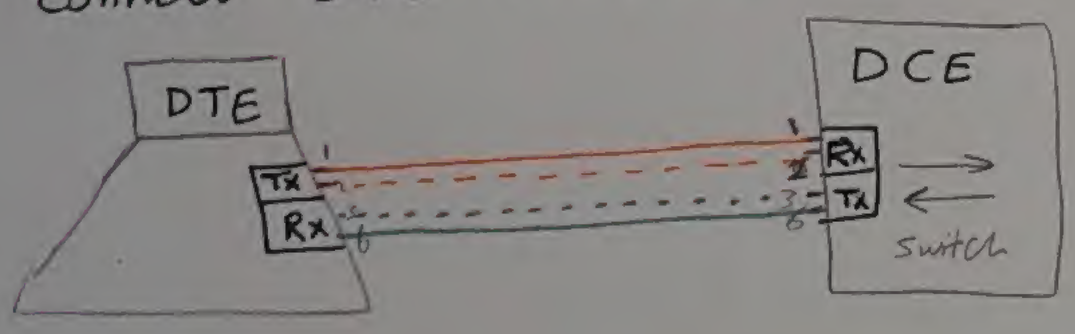
Tx : Pin 1,2
Rx : Pin 3,6
as PC & Router

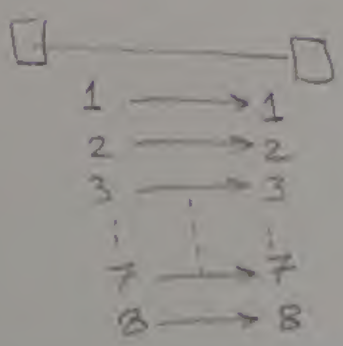
LAN DCE

Tx : pin 3,6
Rx : pin 1,2
as switch & Hub

1 Straigh Cables :-

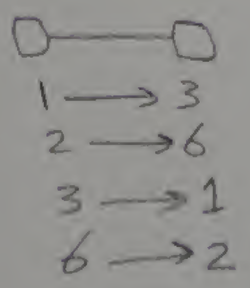
Connect DTE to DCE



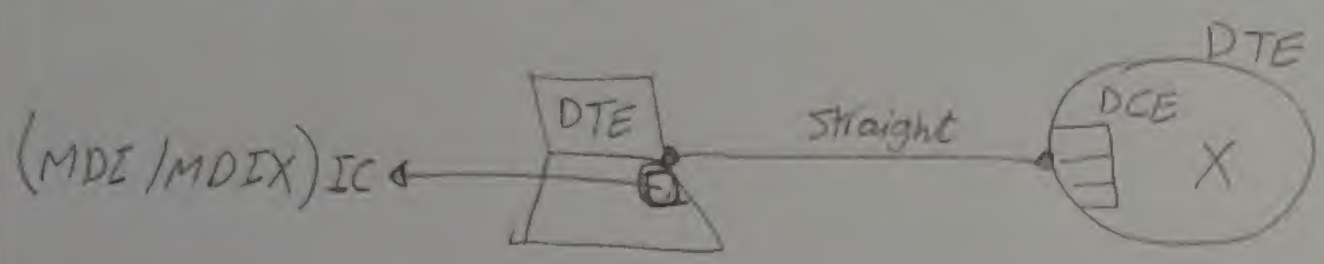


2 Cross cable :-

Connect two DTEs or tow DCEs

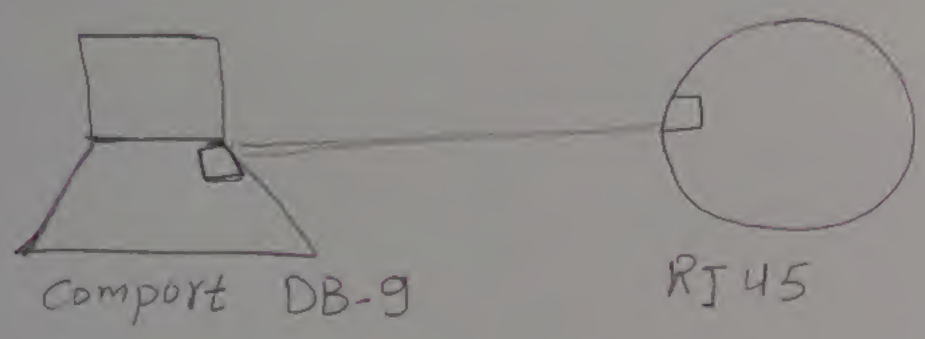


the Router in your home contain a built in switch, so that you can use a straight wire between your computer & Router and also the Router contains an IC that is called [MDI/MDIX] used for autosensing, then there is an option that you can connect the cable whatever you want [straight or cross] and this IC will sense and correct the direction of Tx & Rx signals

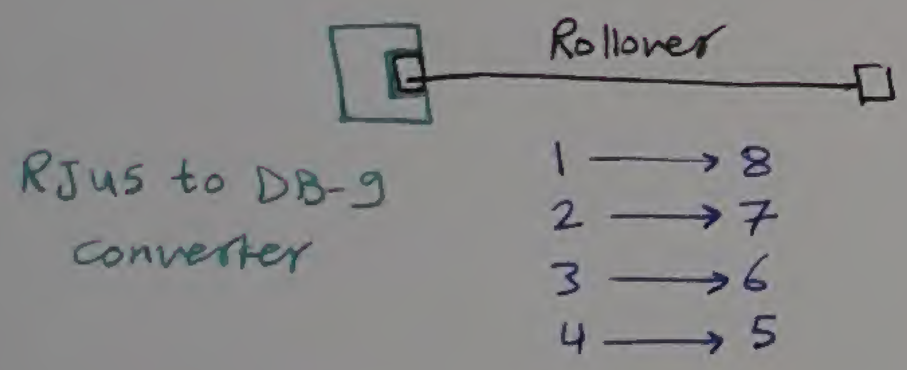


[3] Rollover cable [Console cable]

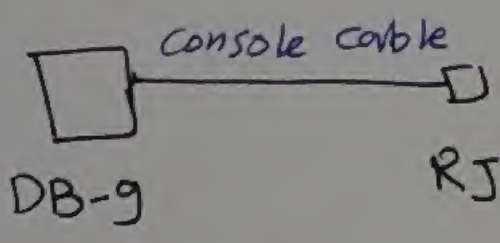
it is used for configuration only not for Data delivery



RJ-45 to DB-9 converter انت محتاج
DB-9 الى RJ-45 عشانه تحول من



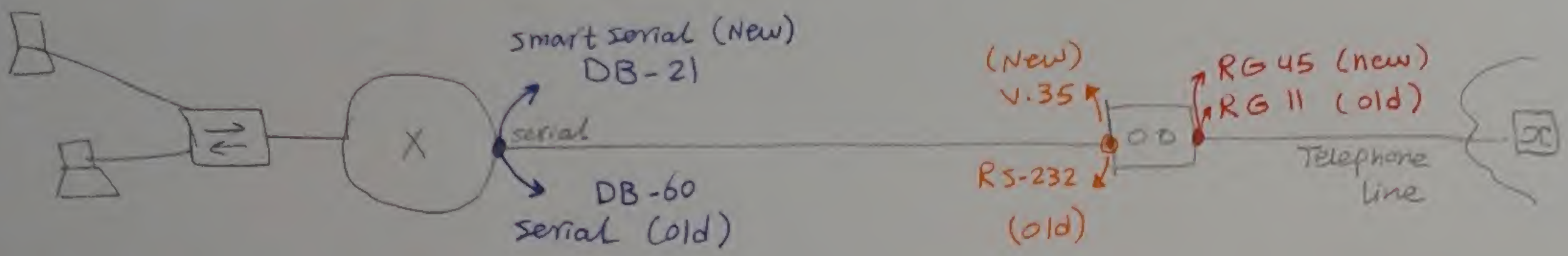
لو محتملة تفصيل
converter + Rollover

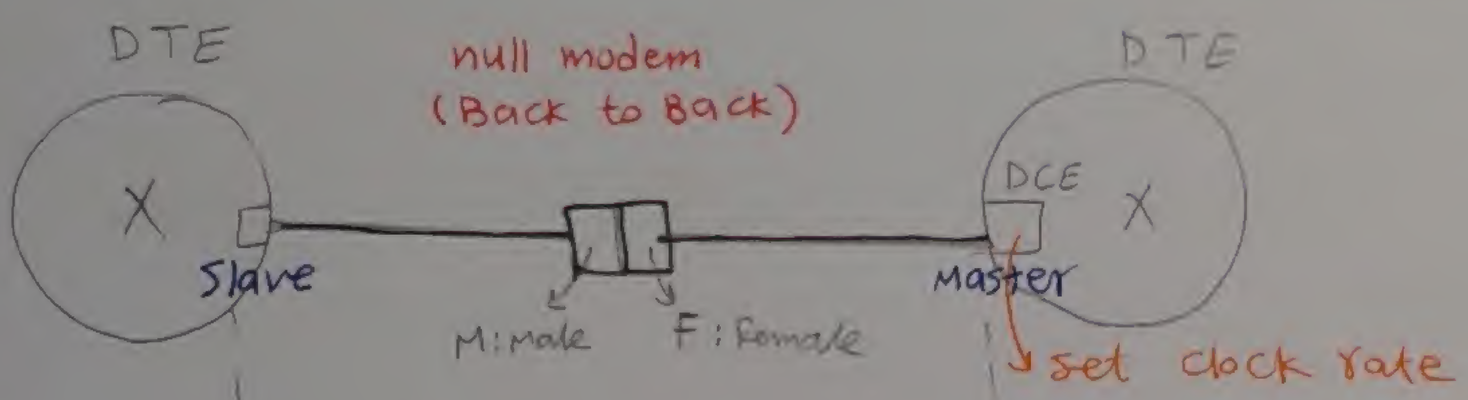


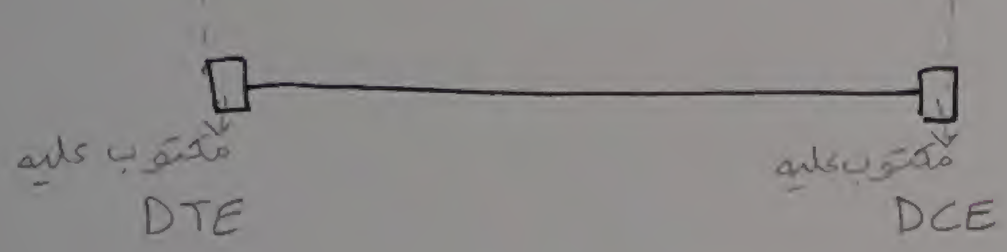
لو مشتريه جاهز هتشتري
console cable

* physical layer

PDU = Bits







الطرف اللي مكتوب عليه DCE

هو الي على الروتر اللي متوصل بيه (DCE)

وهتعمل عليه الـ set clock rate

* physical layer Devices

[1] Repeater

* it regenerates the signal
* I cannot use more than 4 repeaters because of the delay and collition

* max no of ports = 4 ports

[2] Hub

* it is centerelized devica that support star topology ↔ advantage
* it is Multiport repeater ←
* it floods data → disadvantage

[3] Modem

* Data link layer

delivery data & control problems from hop to hop

مسئول عن التحكم في الكونترول وفي نقاياه LAN بتتكلم عن الـ WAN

[I] MAC address :-

[Network interface card]

it is an address that is burnt on NIC Rom , it is 48 bit address represented in hexa decimal , used to send & receive data hop by hop

1 bit hexadecimal = 4 bits

12 ~ ~ = 48 bits

* العينه اللي بتنظم وتعطي ارقام الـ MAC هي IEEE

[organization unique Identifier] OUI ≡ vendor part (24 bit) | host part (24 bit)

XXXXXX XXXXXX

12 bit hexadecimal

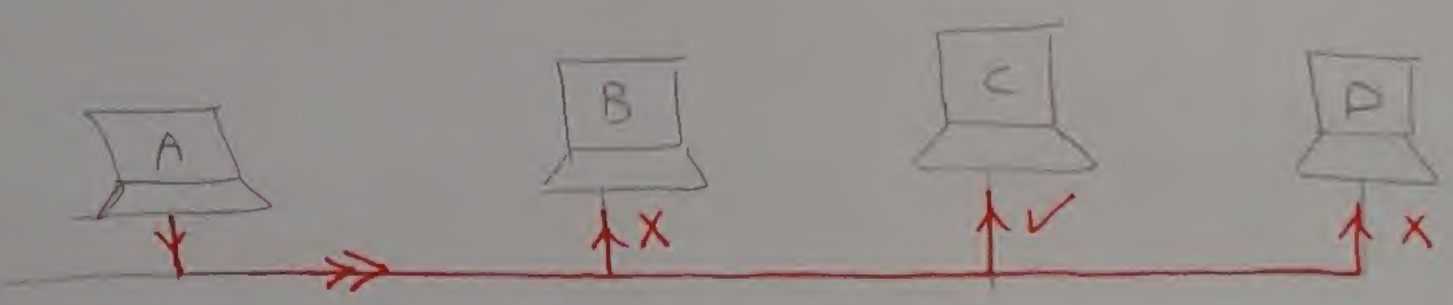
* Cisco has 32 vendor part

Types of destination MAC

[A] unicast MAC

A ⟶ C

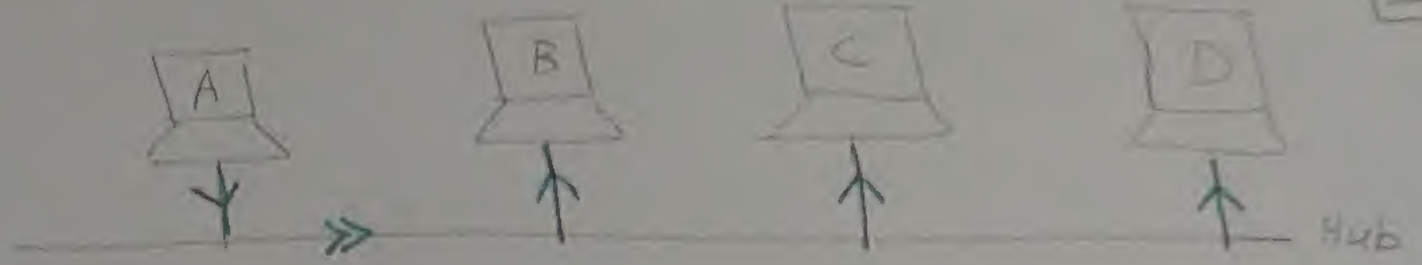
one send & one process



Example of unicast :-

- HTTP ⟶ لأن بـ Browse هو جهاز واحد
- FTP ⟶ بـ DL او UP هو جهاز واحد
- SMTP ⟶ نفس الـ HTTP
-

b Broad cast MAC



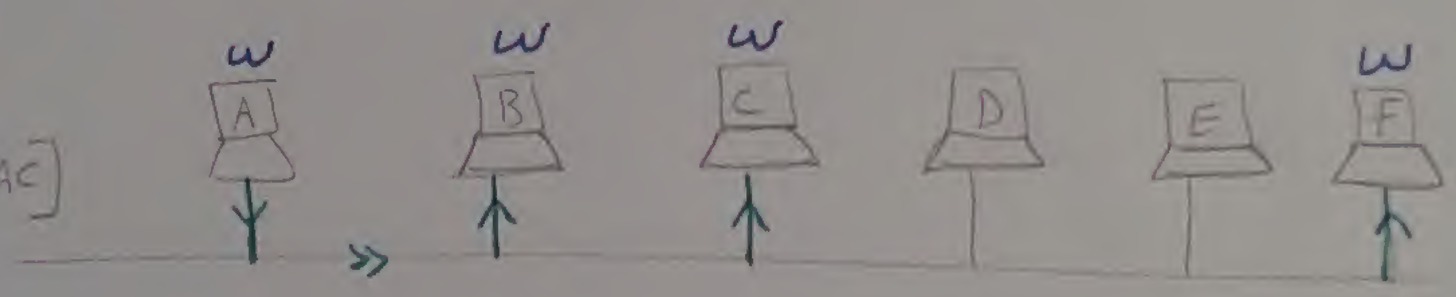
destination
FFFF FFFF FFFF

one send & all receive and process

* Broad cast الـ MAC خليه كل NIC في الـ MAC عام كله FF...FF الـ Broad cast بيبعت

note
* Flood ⇒ all devices receive the data but some only can process
* Broadcast ⇒ all devices receive the data and they must process it
بمعنى انه الـ Broad cast بيجبر كل الاجهزة انها تـ process الداتا

c Multicast MAC [application games]



one send & some receive and process

* اى Multicast application زى الـ Fifa بتروح الـ IEEE وتطلب منها اكتر من MAC معين عشان كل مجموعه بتلعب Game مع بعض ياخدوا MAC address والـ MAC دة بيكون virtual MAC يعنى مبيكنش مطبوع فى NIC بتاع جهازك لكنه الـ application بتطلب الـ Multicast MAC من الـ RAM اثناء الـ Game

then every NIC card has more than one MAC address

1- unicast MAC
2- Broadcast MAC
3- Multicast MAC If you play a Game and If you play 1000 application then you have 1000 Multicast MAC address for them

[2] MAC Method

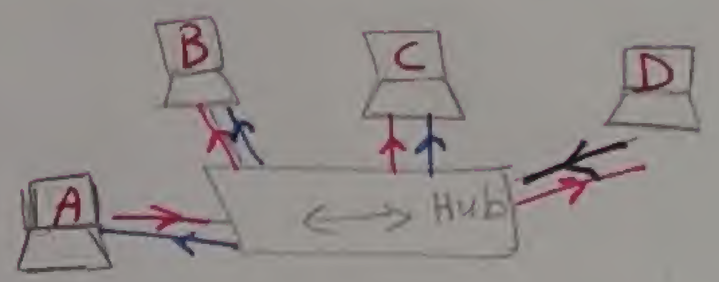
CSMA/CD : Carrier sense multiple access with Collision Detection

* CSMA is the brother of CDMA & TDMA & FDMA and it is the oldest of them
* CSMA is found on NIC
* we use it in case of using the Hub and wireless but we don't use it in case of switch

CSMA يا ريت متستخدمش

If I need to transmitte, first I should sense the receiver
- If Rx is busy ⟶ stop Tx
- If Rx is free ⟶ start Tx

note / all devices on a hub should operate half duplex
[eg either Tx or Rx at atime]

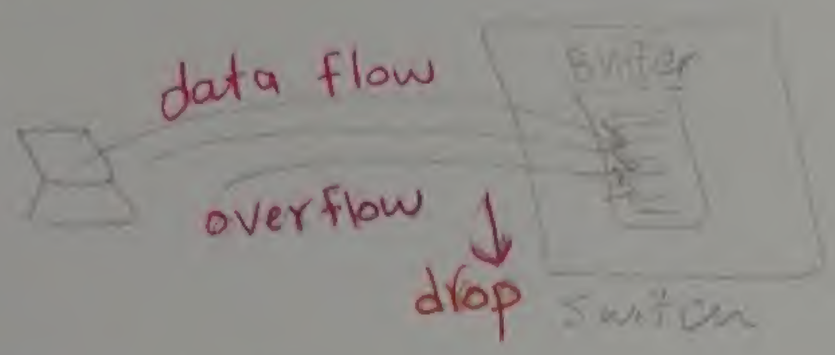


متنفعش في حالة

* IF A & D send in the same time, collision will take place then A & D will be the first to detect the collission because they found themselves can both send and receive
* then A & D will start a back off algorithem [will stop sending]
* A & D send jam signal [إشارة إعاقة] to alarm B & C to the collission to cancel the operation of the sended Frames
* then each device that sensed the collission will start to transmitte in a random time to prevent a new collission again

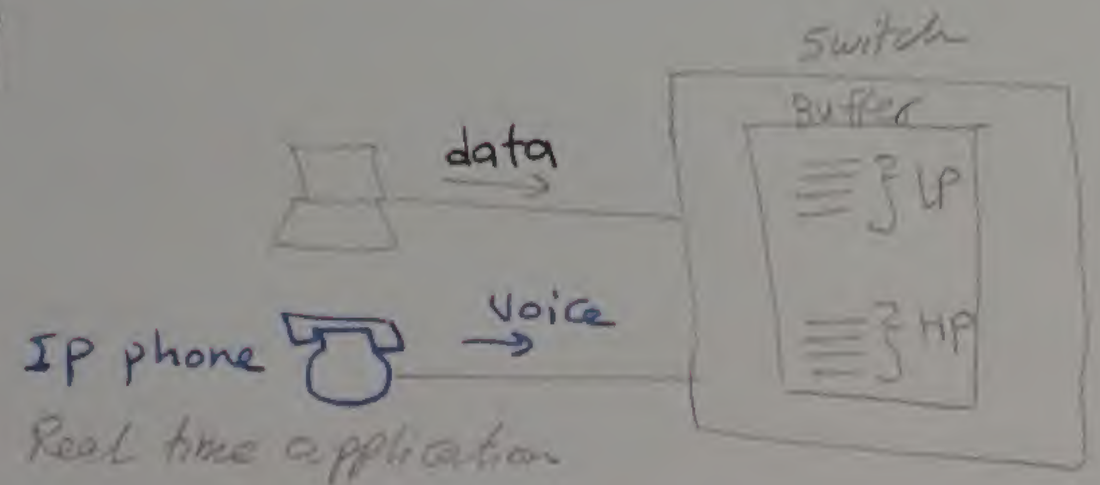
(3) MAC Flow Control

(a) Buffuring



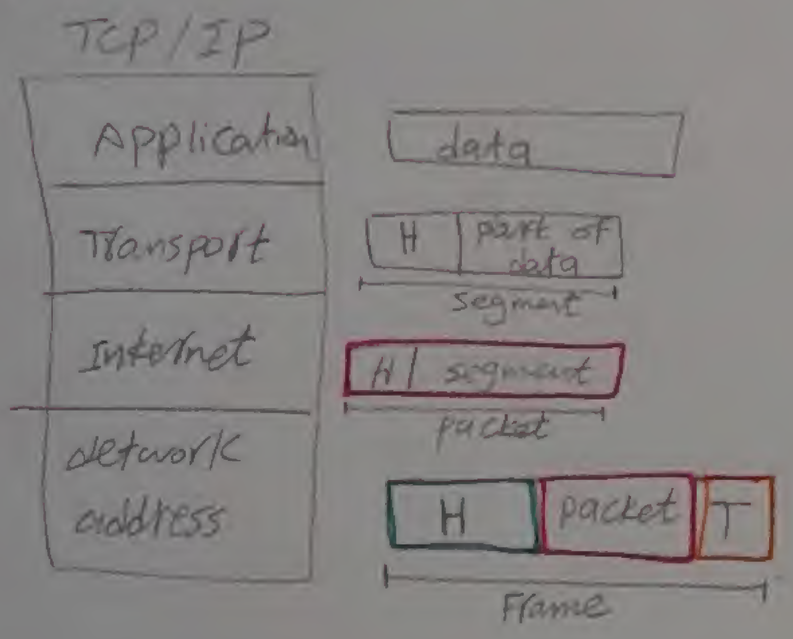
(b) Congestion avoidance تفادي الاختناق

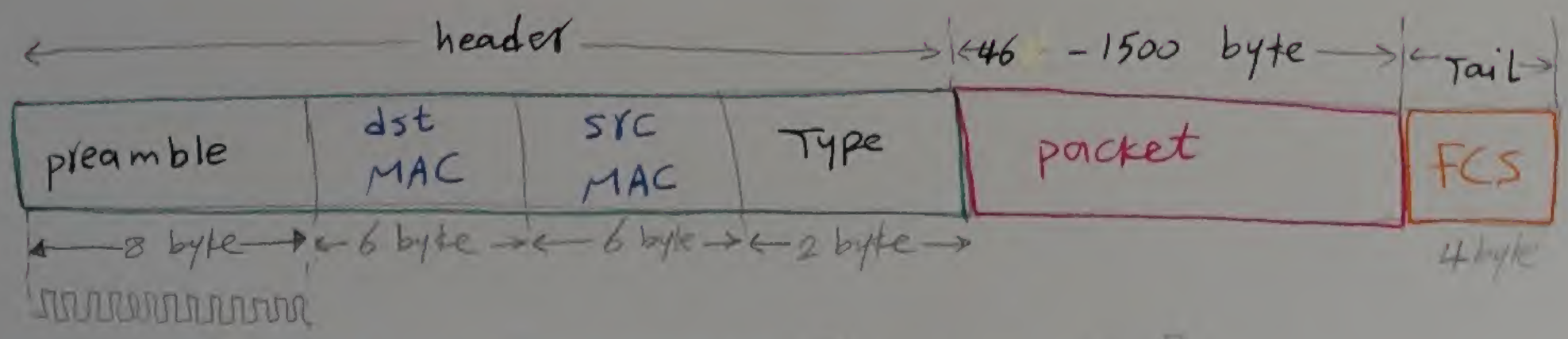
→ drop low periority



- it gives the Data low periority and the voice high periority
- If th memory is full , it deletes the low periority data to serve the high periority voice , because I can resend the data again but I can't resend the voice to be transparent to user

(4) MAC Frame





FCS : Frame check sequance [it is as CRC]

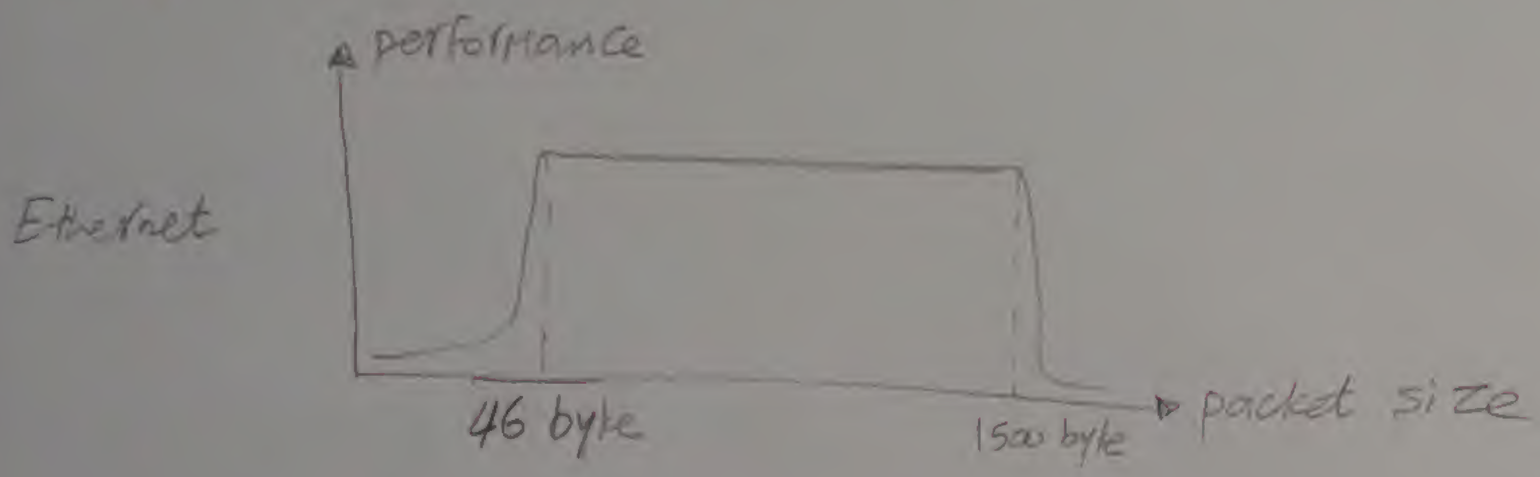
note 1

* the preamble is used to determine the autoclocking

If it is → 100 Mbps / 1 Gbps / 10 Gbps for Ethernet, and it is sent at the start of sending only

not 2

* performance V.S packet size for Ethernet



MTU : Maximum Transfere unit

not 3

type (type) : Contain the name of upper incapsulated protocol

ex: IPV4 or IPV6 or IPX

يعني الداتا جت منين

and also it contains the length of frame

Then the frame size → min → packet + H + T = 64 byte
→ max → packet + H + T = 1518 byte

5 layer 2 devices

Devices understand MAC

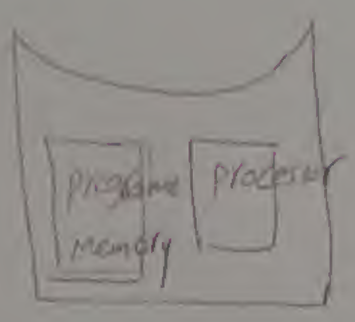
- address
- Frame
- method
- Flow Control

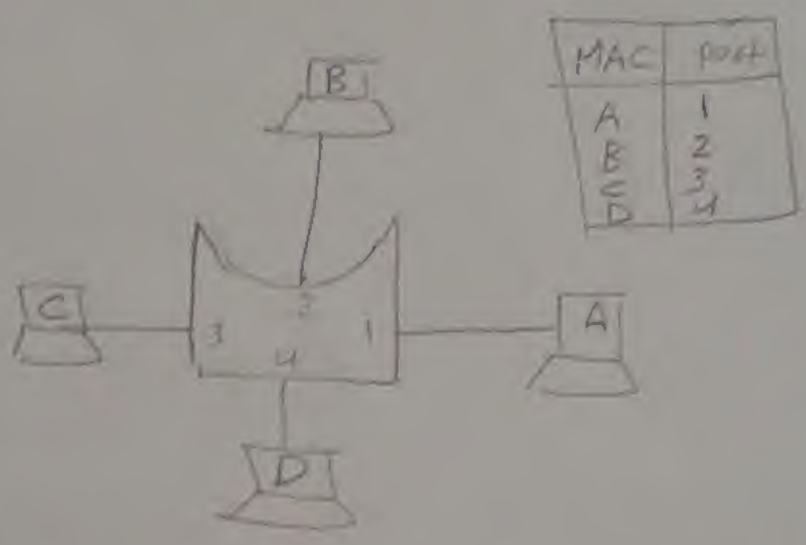
1 NIC: [Network interface card]

→ it has MAC

2 Bridge:

- it acts as intelegent repeater
- it builds a MAC table
- max no of ports = 16 port
  (this no is very limited
  → dis advantage of bridge)
- it operates by S/W

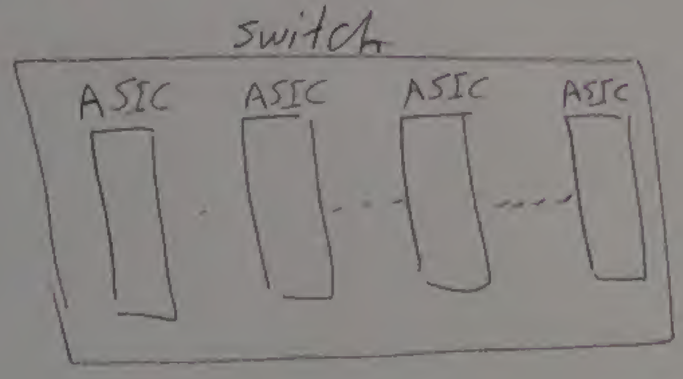




S/W ده الـ Frame بيزم الـ ← Frame كل تنفذ عشان الـ Bridge ده وجود معناه
بتفضها وده بيخلي الـ Bridge بطئ جداً وقلل كمان عدد الـ ports
اللي فيه عشانه الـ Bridge مش بيونج

3 Switch

- it is multiport Bridge
- it operates using HW ASICs [Application specific integrated circuits]



* Each ASIC has a specific Job

Cisco Catacyst 6513
576 port
720 Gbps
↓
1.4 Tbps

Juniber EX-8216
786 port
6 Tbps
↓
12 Tbps

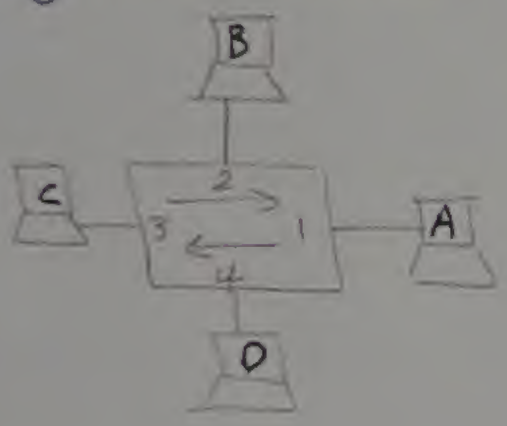
Cisco NEXUS
3xx port
12 Tbps

→ Tera ≡ 1000 Giga

Switch operation → learning through SRC MAC
→ Forwarding through DST MAC
→ Remove L2 loops
↓ layer 2

1 learning

Forming MAC table by checking SRC MAC in any incoming Frame

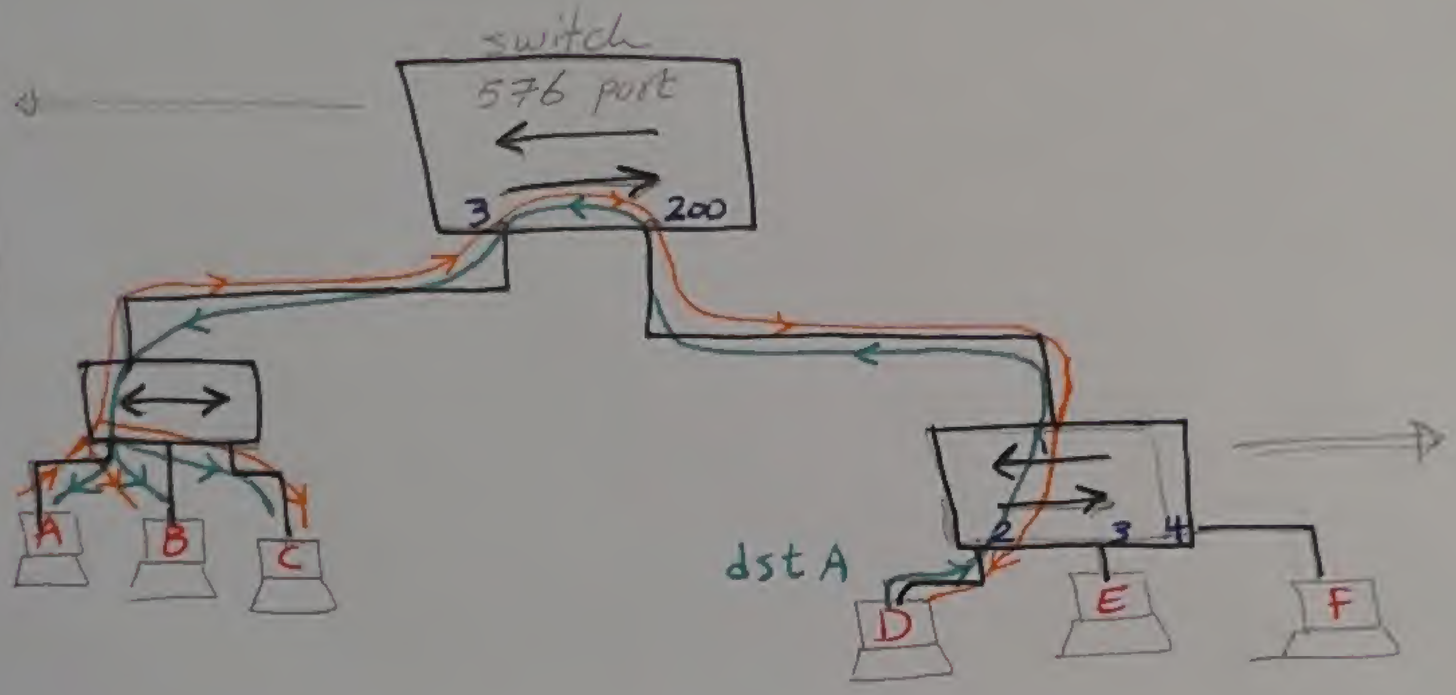


MAC Table

MAC	port
A	1
B	2
C	3
D	4

* the MAC table is in the volatile memory RAM

MAC	port
A	3
B	3
C	3
D	200
E	200
F	200

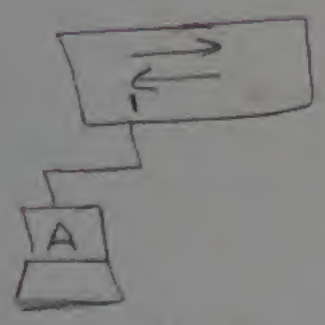


MAC	port
D	2
E	3
F	4
A	1
B	1
C	1

Note A switch can learn many devices on the same port

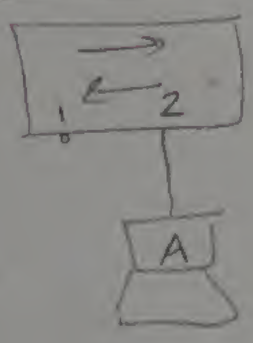
* switch flush (يمسح) inactive entries after 5 mins of inactivity by default
يعني اذا لو ال PC انتقال من ال Network ما ال Switch هيتخزنه من الجدول بعد 5 دقائق

Note B switch will never learn existance of a device in 2 different ports



MAC	port
A	1

after a time



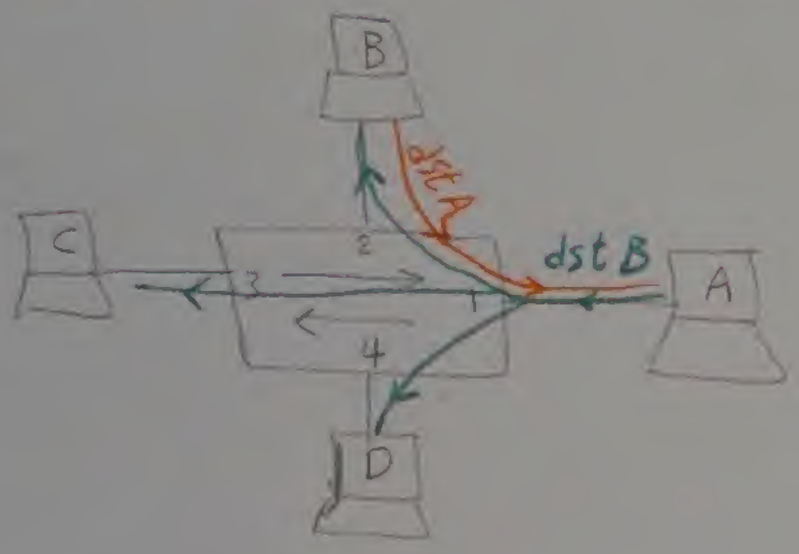
MAC	port
~~A~~	~~1~~
A	2

[2] forwording

switching frames to the next hop by checking dst MAC in any incoming frame

→ switch will flood If dst MAC :-

[1] If dst MAC is unknown unicast :-

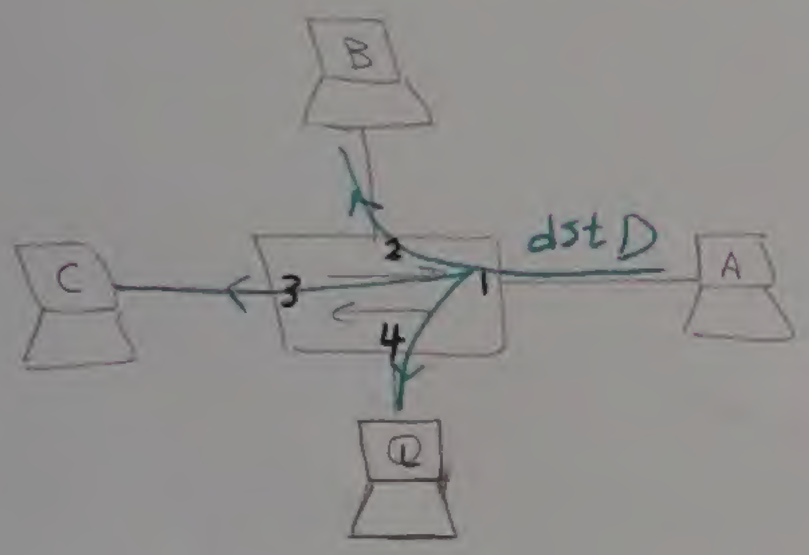


MAC	Port
A	1
B	2

من الحاله دى ال switch هيعمل Flood و تا بس هى الى هتعمل process

[العمليه دى اسمها Handshaking قبل ميبعتوا لبعض]

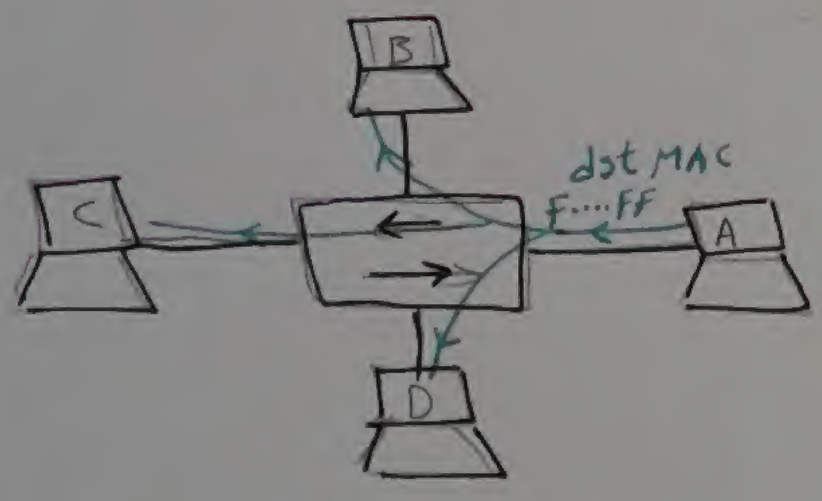
ال switch بيـ Flood عشان يستنى الرد



MAC	port
A	1
B	2
C	3

لو ال switch يعرف الجدول للقابل وبعدين A عايز يكلم D ⇐ فى الحاله دى ال switch تلزم ← Flood على كل ال ports عشان يوصل لجهاز D

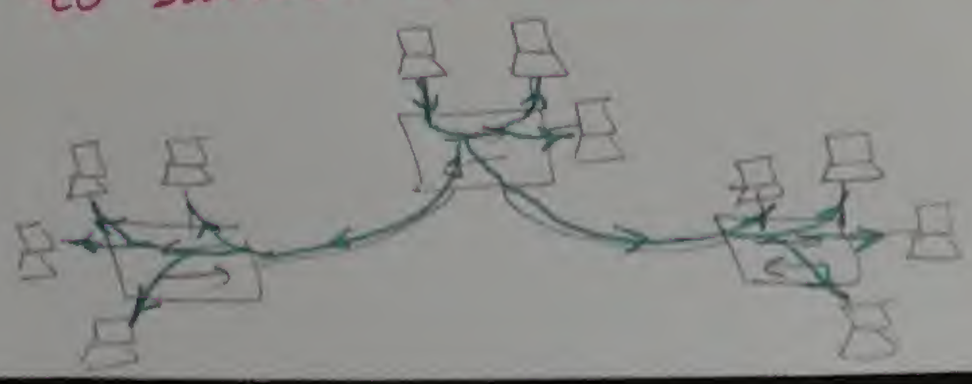
[2] If dst MAC is Broad cast



the switch doesn't broadcast [e.g force the PCs to process the data] but the switch is Flood

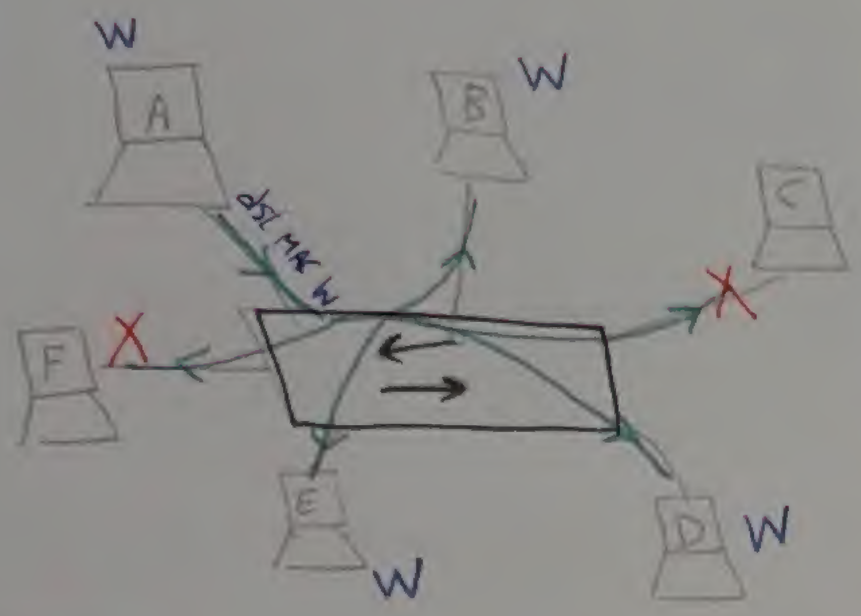
one Broad cast domain

Note < All devices connected to switch are members of a single Broadcast domain



This is also one Broadcast DOmain

3 If dst MAC is multicast [it is used in Games]



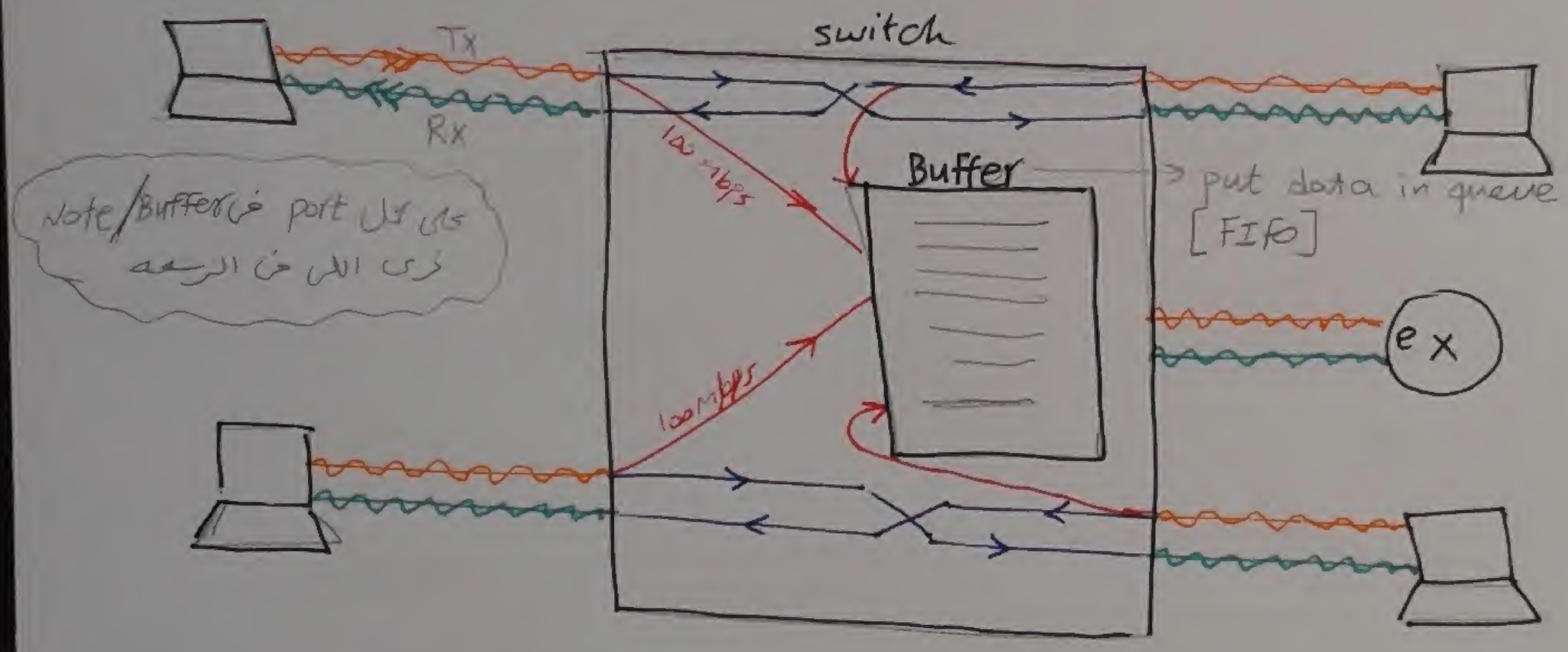
* W من الـ dst بتاع الـ Application
* الـ switch بيـ Flood واللي عايز يعمل process بيعملها

XXXXX XXXXX
Vendor Host

Multicast Appl. 0/9 ←

Note The main adv. of switch in Flood process that differ it from hub that there is no collission while flood process

To avoid collision :- switch will forward using concept called Micro segmentation

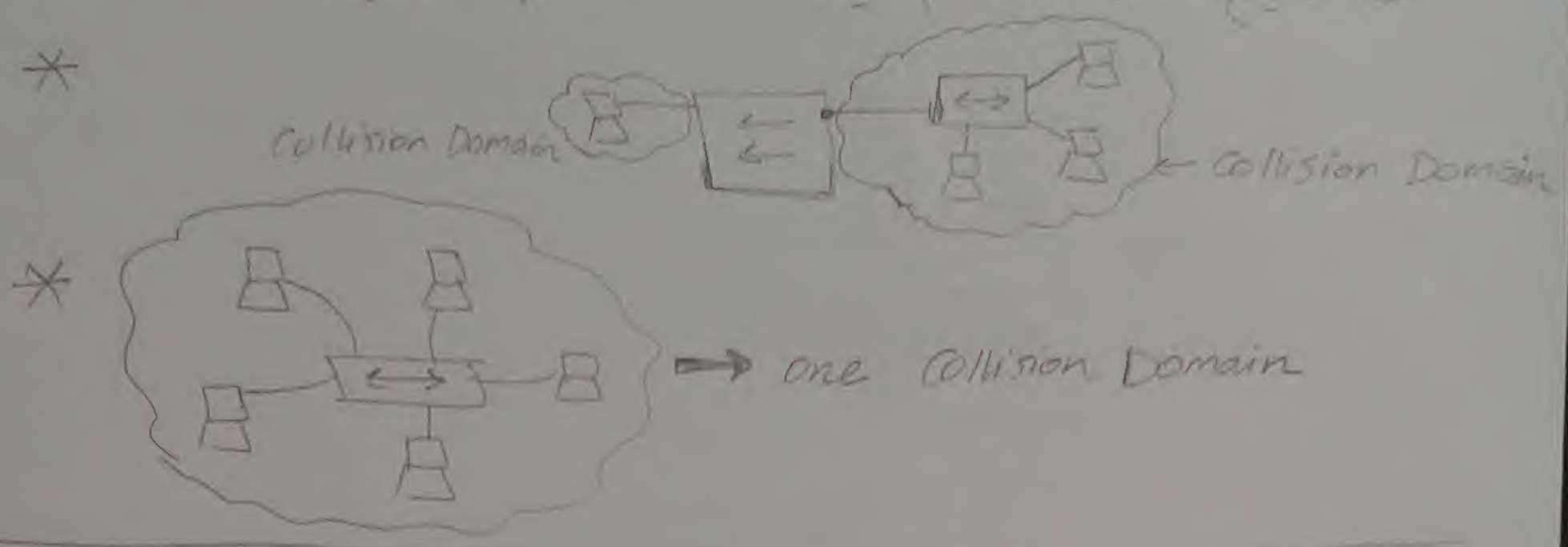


Note D All devices connected to aswitch can operate in Full duplex [can both Tx & Rx at the same time]

* لكنه الـ Hub بيستخدم الـ half duplex عن طريقه الـ CSMA/CD
  - الكمبيوتر هو اللي بيشغل الـ CSMA/CD ← صنا السؤال انه هل الكمبيوتر بيعرف انه اللي امامه switch ولا hub
  - ← الاجابه / الـ PC بيبعت اشارة مش بيفهمها غير [layer2 device] ← لو الاشارة رجعت للـ PC هيفهم انه في switch وهيشغل الـ SCMA/CD ولو جتلش ولا الـ PC ← ← ← Hub وهيشغل الـ SCMA/CD

Note E Each switch port is a separate collision domain

(كل ما يتم حدوث تعارض بين ال ports وبعض)



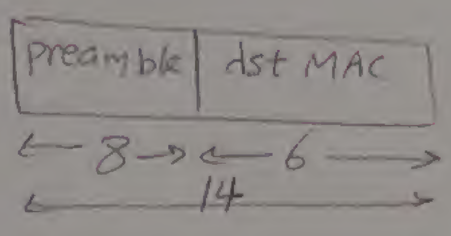
---

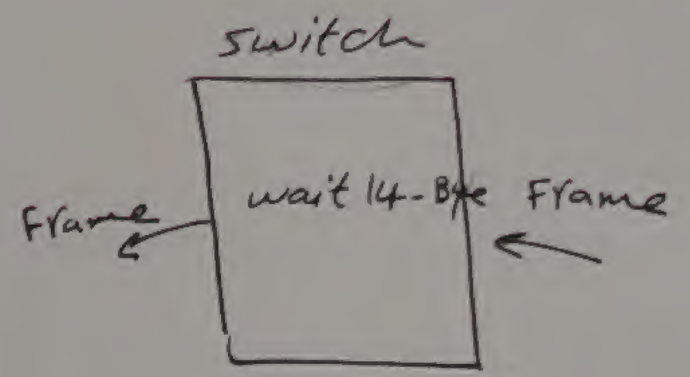
switch forwarding modes (types) :— ≡ switching types

1 Cut through : (سريع اوى لكنه بيعدى ال errors)

wait after 14-byte then forward

↳ to check dst MAC





(ال switch دى بتستخدم فى الشبكات الصغيرة فقط)

---

2 Fragment free (تنقية)

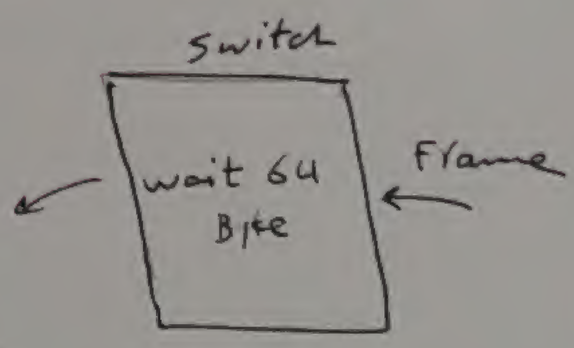
wait after 64-byte then forward

64-byte is the minimum Frame size

* بتستخدم ال switch لما يكون عندك فى الشبكة Hubs

Collision عشان يقدر يعرف ال wireless access point &

* مش بيعدى الا ال Frames الصحيحة



---

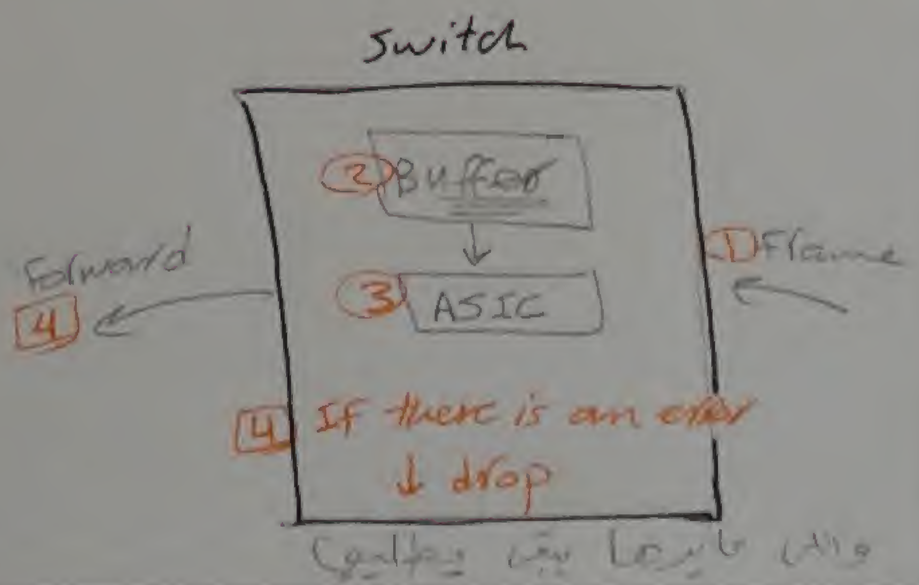
3 store & forward :

(عيبه انه بطئ)

switch stores the full frame and check If there are any errors then forward

error types

- CRC errors
- Runt errors (Frame < 64 byte)
- Gaint errors (Frame > 1518 byte)



(والى تاريها بيتم بطريقتين)

Store & Forward switch ⟹ Detect the error and drop it
it cannot correct the error
الى بتجيلو عشان يعمل check لل Frames ← اذى

[4] adaptive cut through : by Cisco store & forward و cut through بين

starts as cut through untill the error Frames reaches a big no threshold, then changes to store & forward untill errors Frames reaches a small no, then return back to cut through

① cut through If no errors
② store forward If high errors
③ cut through

---

switch operation [continue]

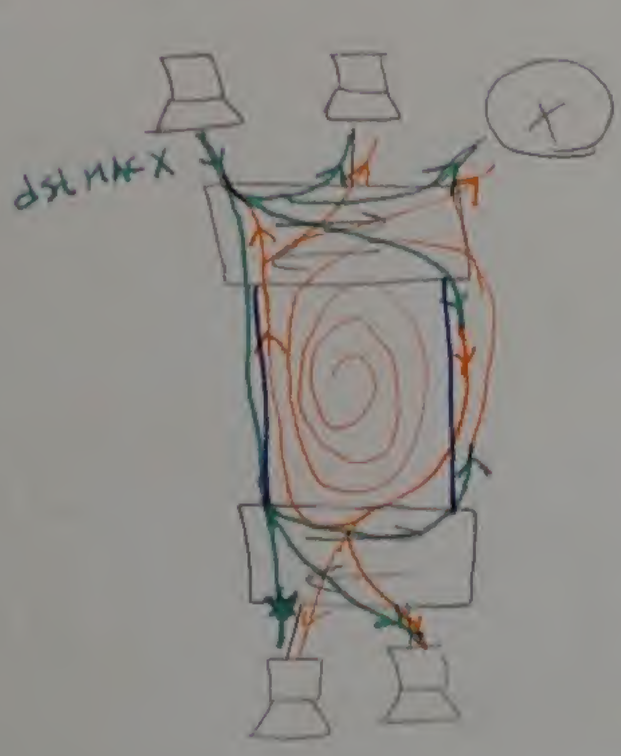
[1] learning
[2] forwarding
[3] Remove L2 loops :-
↓
STP (Spanning Tree protocol)

Rule For TCP/IP: each interface has L2 and L3 address
L2 ↙ MAC L3 ↓ IP

L2 address is address transport the data from Hop to Hop ← one type of L2 address is MAC

-	Comm. Tech.	L2 address (hop to hop address)
LAN	Ethernet wifi	MAC address MAC address
WAN	X.25	X.25 number
	Frame relay	DLC [Data link circuit ID]
	ATM	VPI / VCI virtual path ID / virtual circuit ID

⟸ this table is some of L2 addresses



we connect between the two switches by two wires (كابل)
to sure redundancy

* المشكلة انك لو عملت Broadcast ممكن يعمل Broadcast storm
* الحل في STP انه بيخلي كابل من الكابلين خول (Stand by) link
يعني اكنه مش موجود ولو كابل انقطع بيشغل الكابل التاني

* L3: Internet layer :- for end to end data delivery

it is responsible for

[1] logical addressing : slw address ← Network part / Host part

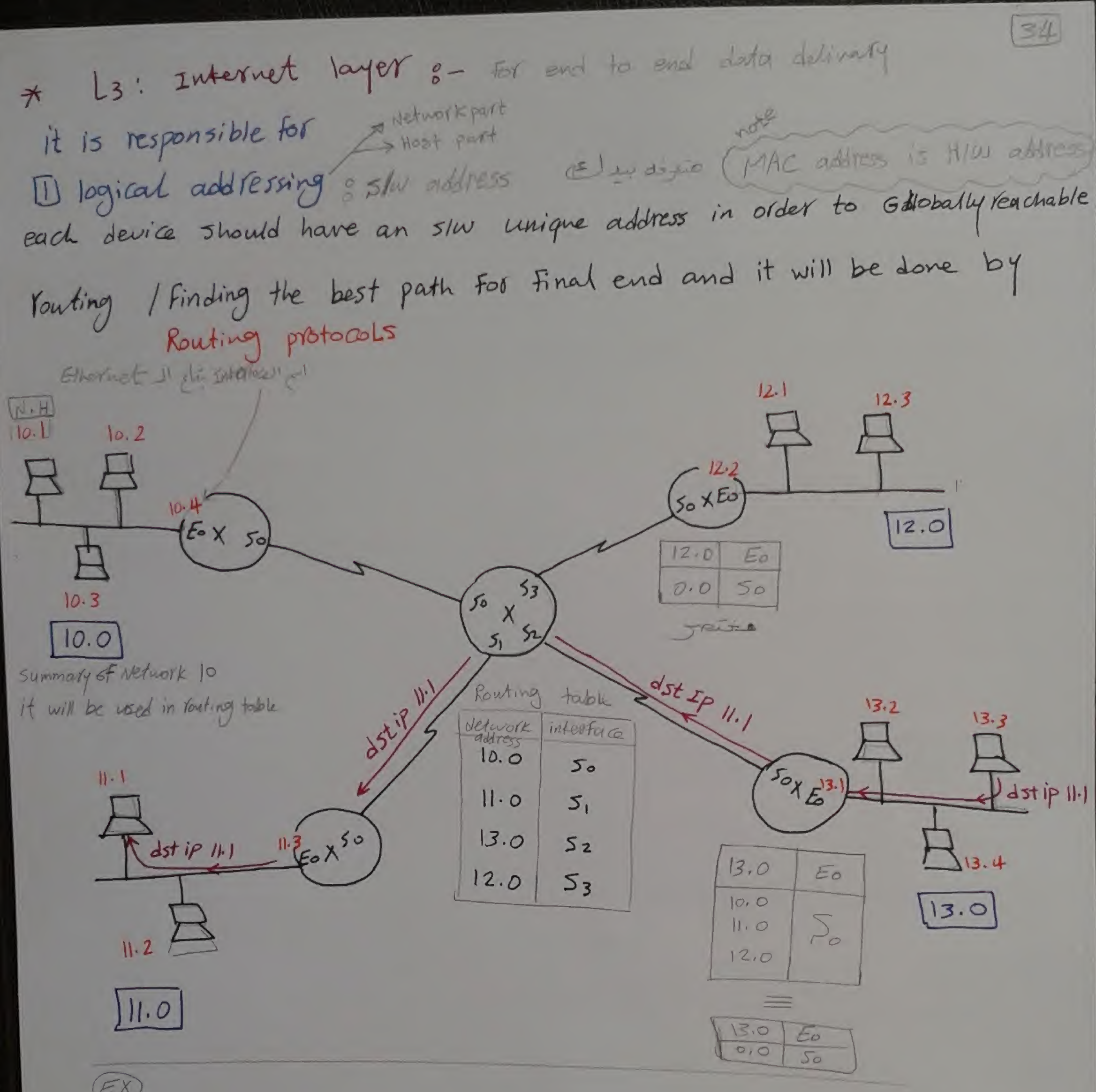
note: MAC address is H/w address (متروك بيدلع)

each device should have an slw unique address in order to Globally reachable

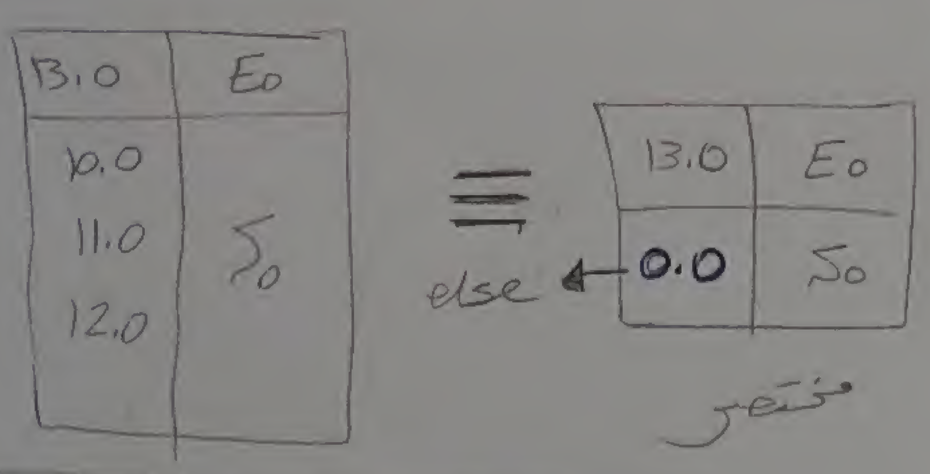
Routing / finding the best path for final end and it will be done by

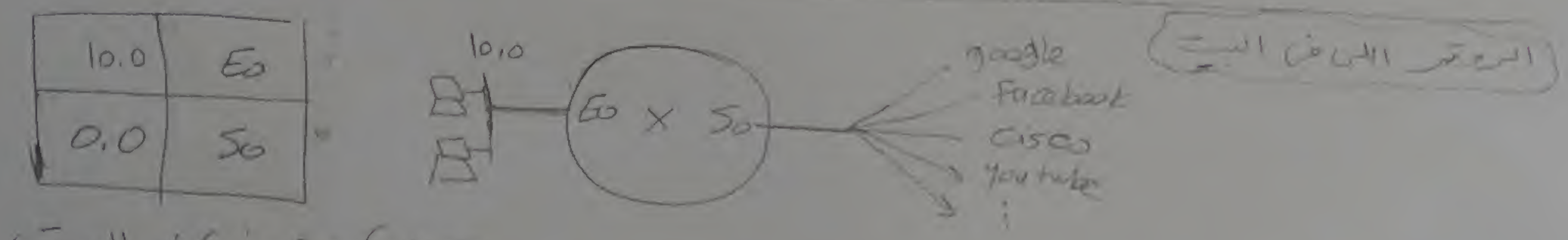
Routing protocols

اسم الانترفيس بتاع الـ Ethernet



EX





switch operation

[1] Learn : Form MAC table by checking src MAC

[2] Forward : Compare dst MAC to MAC table

- If dst MAC is known ⟶ Forward
- ~ ~ ~ ~ unknown ⟶ Flood
- ~ ~ ~ ~ Broad cast ⟶ Flood

Router operation

[1] learn : By forming routing table formed by slw called Routing protocol

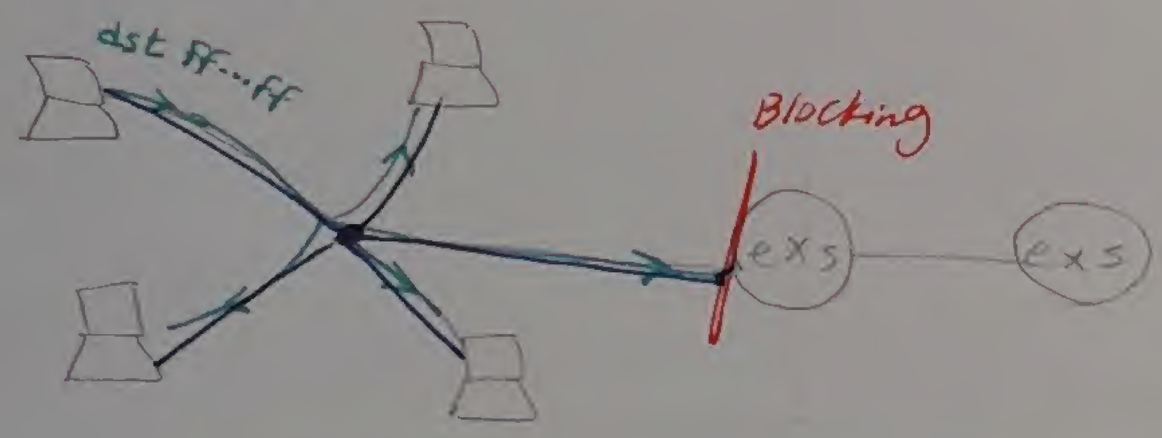
↳ ex : RIP^{V_1,V_2}, OSPF, BGP
IGRP, EIGRP, ISIS

[2] forward : By checking routing table

- If dst is known ⟶ Router will send the packet to the best path.
- If dst is unknown ⟶ Router will drop data

* Router should learn before forwarding

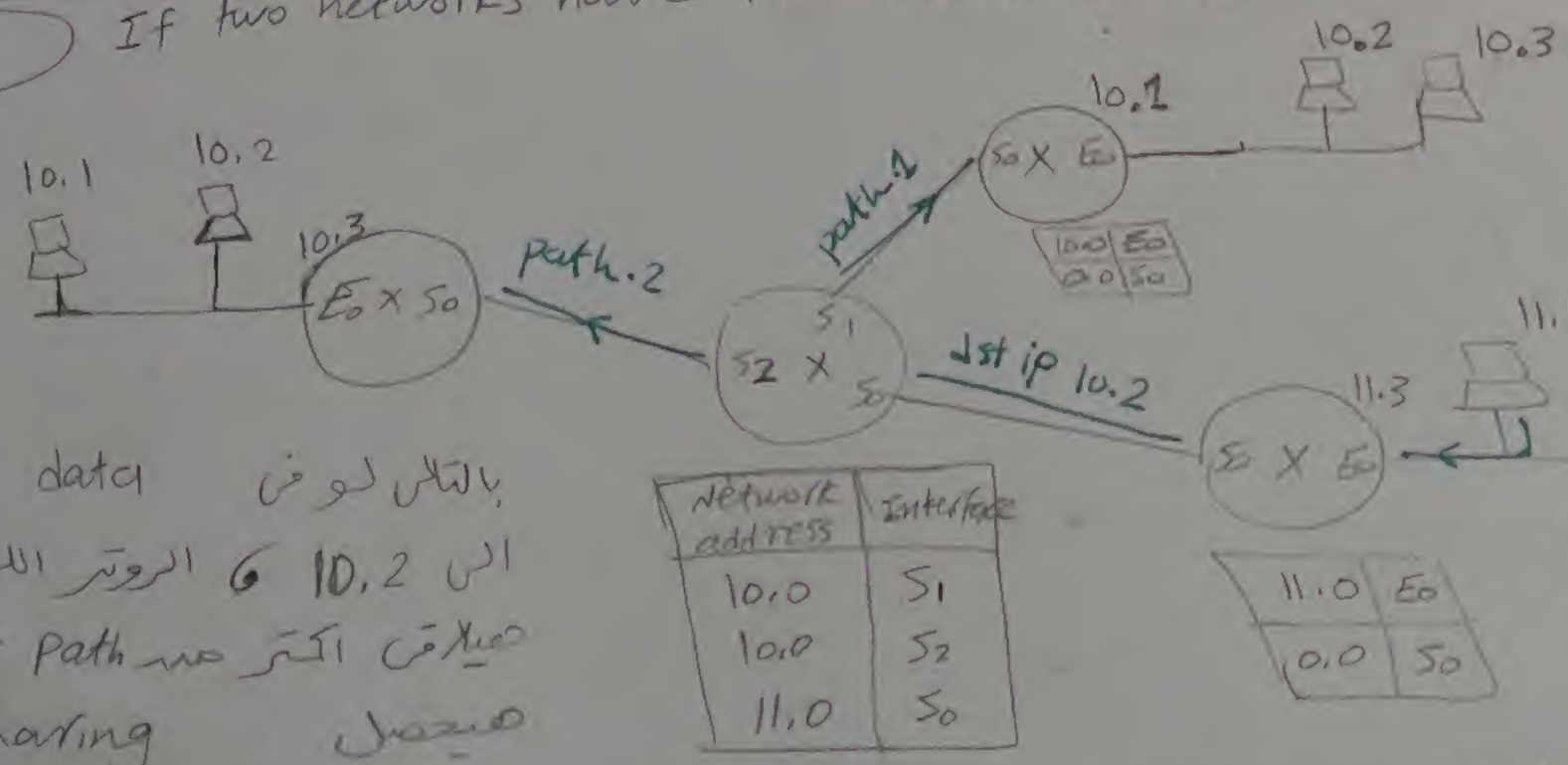
- If dst is Broadcast ⟶ Router will take packet to itself



* The router make Blocking of Broad cast and doesn't pass the data behined itself

---

note If two networks have the same name 10.0



11.1 من جاية data بالتالي لو فى الروتر اللى فى النص الى 10.2 و هيلاقى اكتر من best path وبالتالى

- load sharing هيعمل
- load Balancing ⟶ send packed on path 1 & next packet to path 2 & so on والعكس صحيح

* layer 3 protocols :-

ex: IP V4 : internet protocol

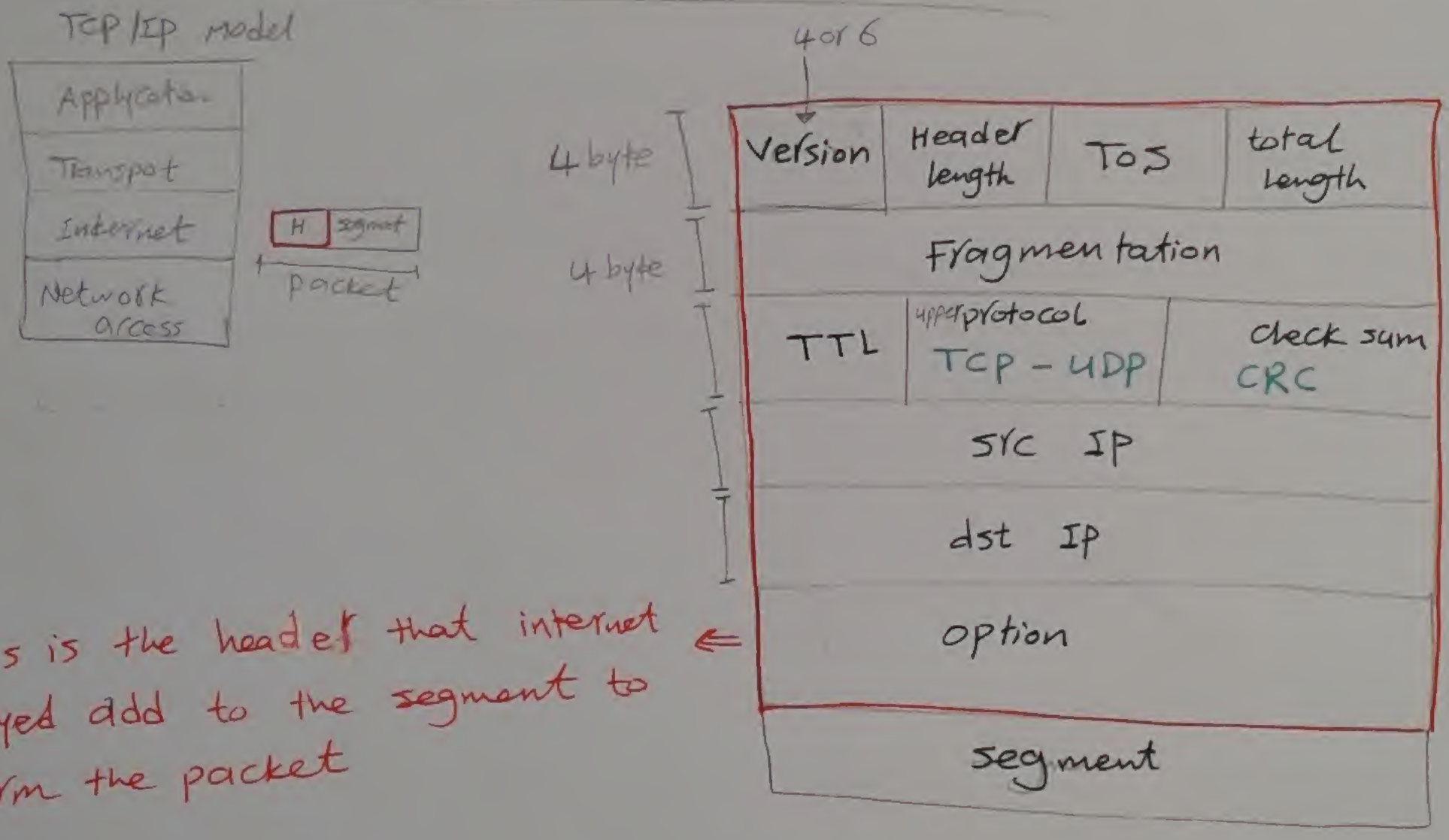
responsible for :-
- logical addressing by using IPv4 address
- end to end encapsulation [delivery] ⟶ IP V4 packet

IP V4 addressing ⟶ 32-bit represented in dotted decimal

10101010.11110000.10111001.10111111

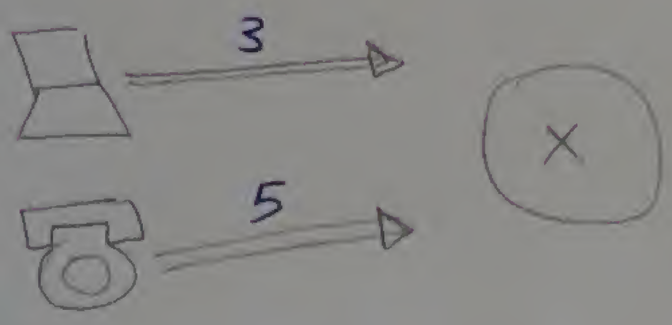
8bit ≡ byte ≡ octet

ex : 170.20.5.192



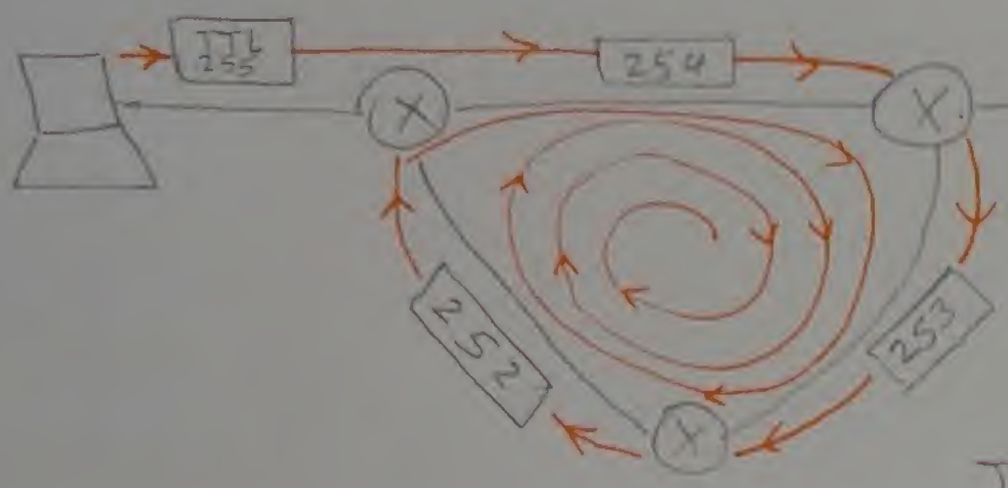
* ToS : type of service ⟶ reflect periority [the highest the number the highest the periority]

it is 3 bits → 0 000, 1 001, ⋮, 7 111



0 1 2 3	data
4	vedio
5	voice
6	Router protocol
7	switch protocol

TTL : time to live it is 8 bits [0—255]



* كل ما الـ packet بتعدي على Router
← الـ Router هينقص 1 من خانه الـ TTL
* لو الـ Router شاف الداتا في خانه الـ TTL = 1 ⇐ هيعرف انه الـ Data دي بتعمل loop بمعانا فترة كبيرة قدرها 254 مرة وهياخد القرار انه يرجعها
⇐ العملية دي بتحصل لأن في الحقيقة عشان توصل لأي Router في العالم بتعمل عدد hops قليلة لا تتعدى 20 hop على 20 Router حول العالم

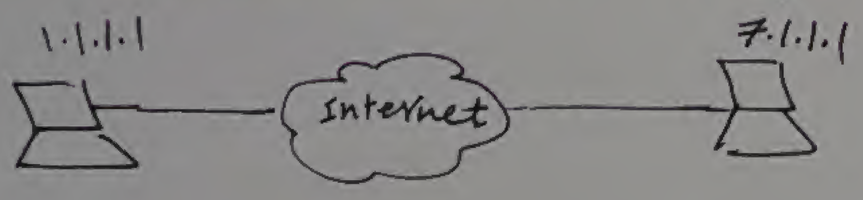
---

* ازاي نعمل check على end to end عشان نتأكد انه الـ Data بتروح من end الى end
* Troubshooting protocol from end to end

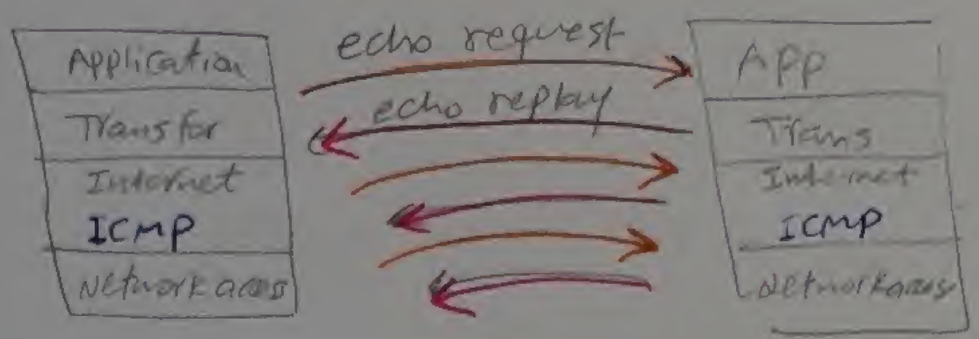
ICMP [internet control messaging protocol] موجود في Internet layer
يعالج مشاكل — using message

البروتوكول دة شغلته انه يبعت رسايل للـ end ولو رجعت ارساله يبقى الدنيا شغاله

I] echo request & echo replay msg :-



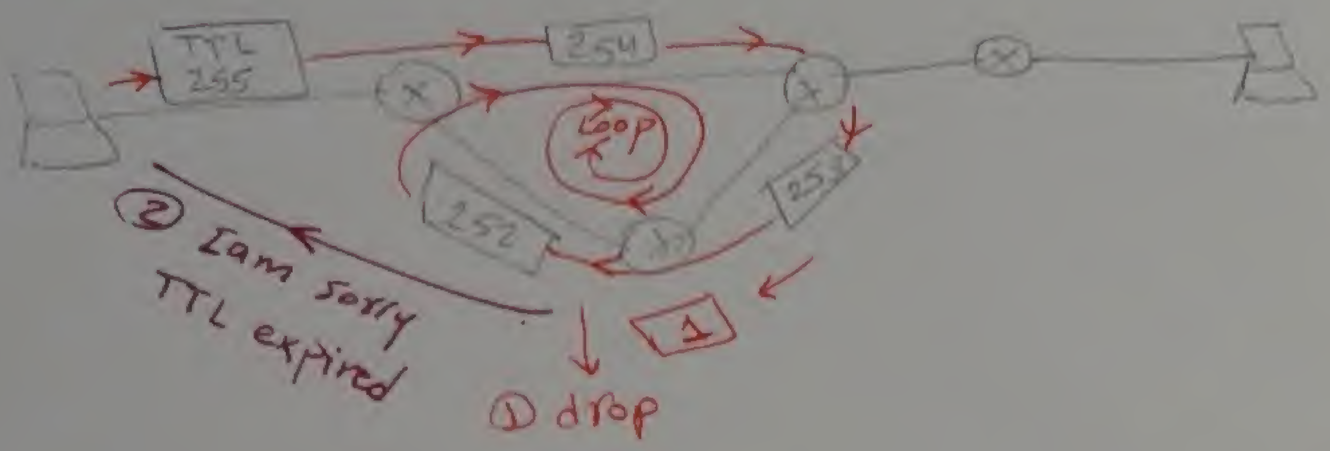
افترض انك على جهاز 1.1.1.1
و عايز تبعت request للجهاز 7.1.1.1 عشان تتأكد انه شغال وهيقدر يتواصل معاك
فهتعمل Command بسيط اسمه ping 7.1.1.1
لو 7.1.1.1 شغال هيبعت رد عليك وبالتالي انت هتعرف انه شغال



windows يعمل ← 4 echo
IOS ← 5 echo
linux ← ∞ echo

* بعد ما بتعمل امر ping 7.1.1.1 ⇐ الـ pc بيقولك الـ Data بتروح وتيجي بعدين تمام ٪

② TTL expiration message



ويندوز ١ → PC → Start → Run → CMd → Trace www.FB.com

على الـ DOS

لاحظ انت ممكن تعمل ping www.fB.com

Session 8

- الهيئة المسؤله عن توزيع الـ IPs اسمها IANA

IPv4 Classes :-

Fixed ↓ Variable ↓

[1] Class A N.H.H.H

EX 57.X.X.X → summary of some devices

57.0.0.0 (Network address)

57.255.255.255 (direct Broadcast) used for appl. & protocol

These two IPs don't be used as IPs for end devices

First octet : 1 ⇝ 126

[2] Class B N.N.H.H

First octet : 128 ⇝ 191

[3] Class C N.N.N.H

First octet : 192 ⇝ 223

Note Each interface [DTE] should have either Class A or B or C address

[4] Class D reserved for multicast application

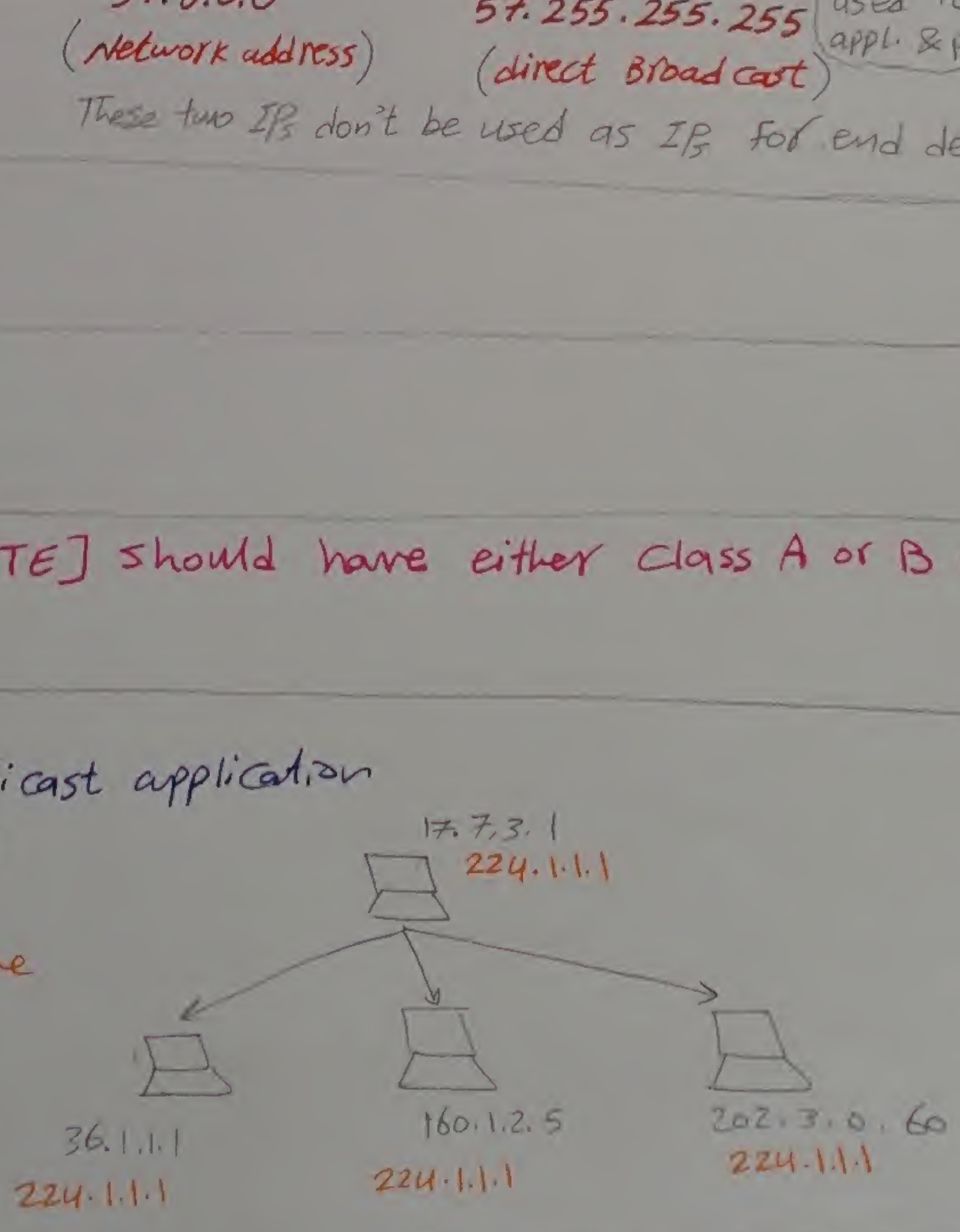
First octet : 224 ⟶ 239

this is vertual IP

(244.1.1.1) is Extra address that the application give to you

⇒ this IP is burnt in the RAM

يتم تحويل الـ MAC الى IEEE الخاص

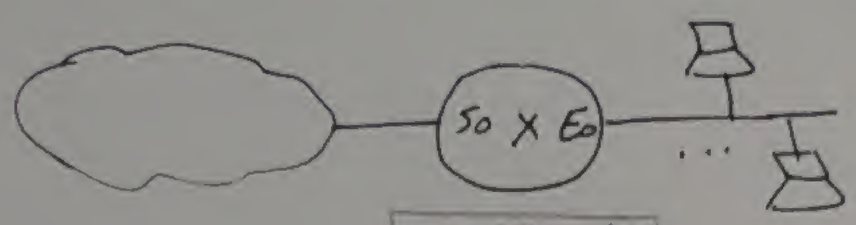


Class E : used for Experements and recearches

First octet : 240 — 254

Classless IPs :-

[A] 0.0.0.0 - it is the sammary of all networks [IPv4 Networks]
- it is used in routers tables



[B] 127 → used for loopback test [self test] ⇒ يعني لو عايز تـ Test الروتر او الـ Pc بتاعك

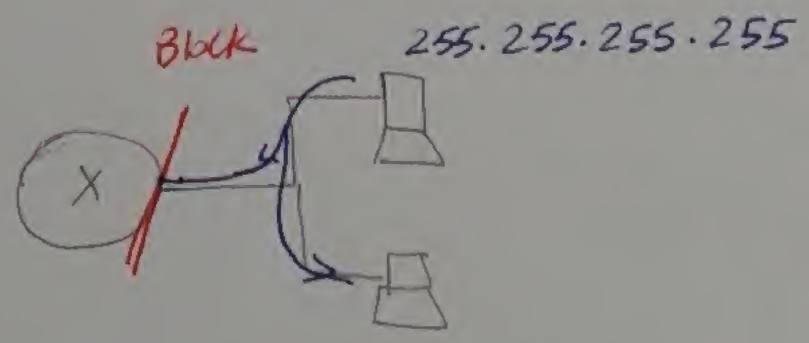
127.0.0.1 used for TCP/IP test ⇒ عشان تتأكد انه الـ TCP/IP بتاع الجهاز بتاعك شغال

Command on the DOS ⇒ ping 127.0.0.1

[C] 255.255.255.255

- Local Broad cast

كل كارت من كروت الـ Network بيقى فيه unicast IP خاص بالكارت + الـ IP بتاع



255.255.255.255 → non Routing

57.255.255.255 → Routable

هنا الـ Router بيعمله process ومش بيمرره بعدة

→ used for applications and protocols

* Classifaction of IPs

EX.1 57.0.0.0 [Network address] eg [summary of some devices]

57.0.0.1 ⋮ 57.255.255.254

Hosts = $2^{24} - 2$

no of IPs = 2^{24}

no of hosts = $2^{24} - 2$

57.255.255.255 ⟹ it is used for App & protocols for Network 57 only

دة عنوان كل الاجهزة اللى فى Network اللى عنوانه 57 بس
يعنى لو فى شبكه عنوانها 63 مثلا و مش هتستقبل العنوان دة

255.255.255.255 ⟶ دة عنوان كل الاجهزة فى العالم

EX.2 191.16.X.X

191.16.0.0 ⟹ Network address [Summary of this Network]

191.16.255.255 ⟹ direct broadcast

no of IPs = 2^{16}

no of Hosts = $2^{16} - 2$

EX.3 192.168.1.X

192.168.1.0 ⟹ Network address

192.168.1.255 ⟹ direct address

no of IPs = 2^8

no of hosts = $2^8 - 2$

* IP V4 Shortage :-

Network need IpV4	Class ??	wasted IPs ??
6	class C [256 IP]	250 IPs
536	class B [65536]	65000 IP
300,000	class A [16,xxx,xxx]	16.xxx.xxx

* solutions :-

1. IP V5 : 64 bit address
2. IP V6 : 128 bit address $\simeq 5 * 10^{28}$ IPV6 / human

---

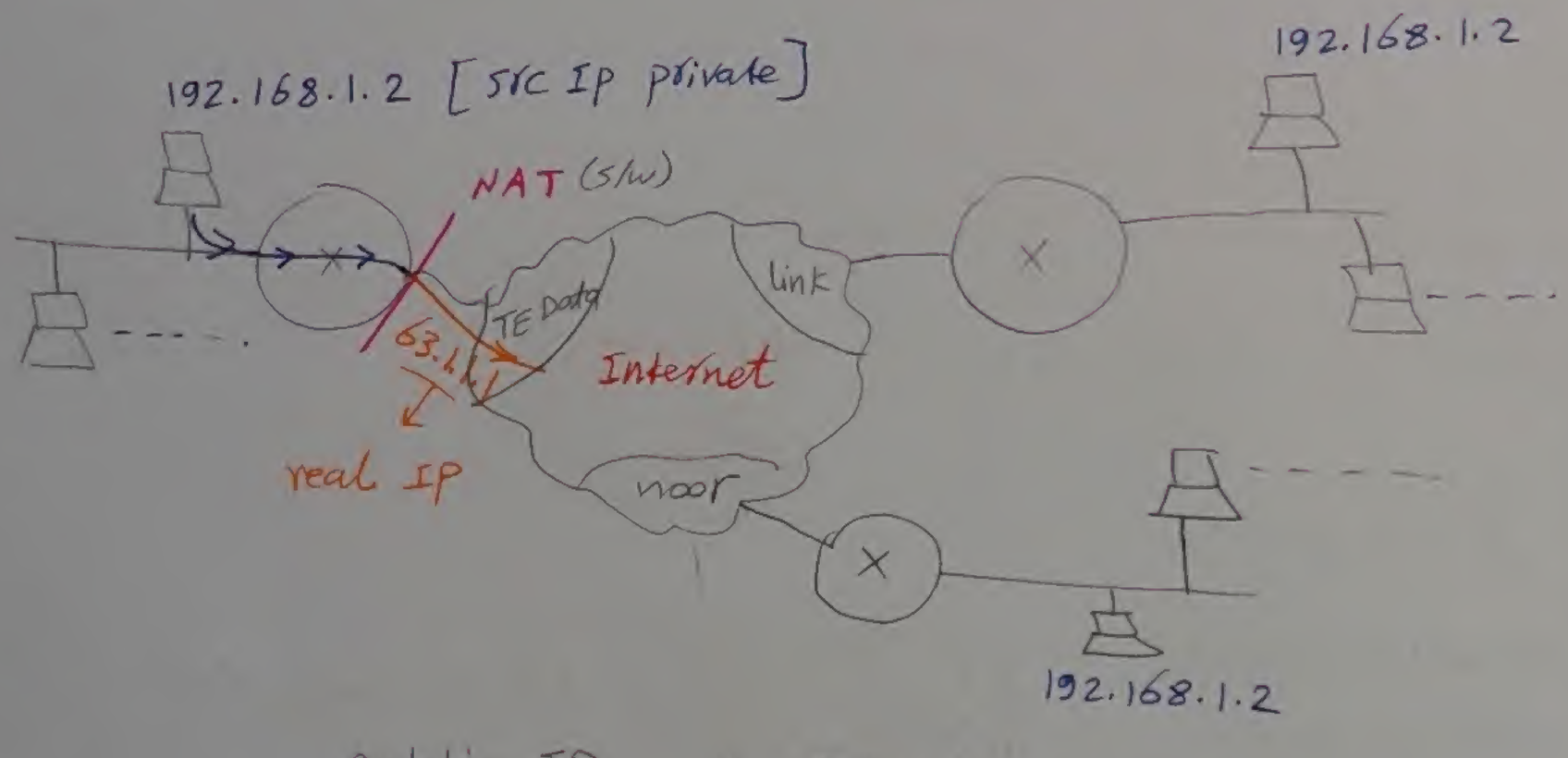
* private IPs + NAT (Network address Translation)

* any one can use the following IPs without registeration but For private use only

10.X.X.X

172.16.X.X ⟶ 172.31.X.X

192.168.0.X ⟶ 192.168.255.X



NAT ⇐ S/W بيحول الـ private IP الى public IP

بيقلل اكتر من private IP بيشيروا لـ one public IP

Subnetworking: it is deviding major network in to smaller networks called subnets

* subneting is done by borrowing part of Host bits & give them to network part

200.1.1.0 } Subnet 1
200.1.1.7
200.1.1.8 } subnet2
200.1.1.15

* مبترجش هنا ان كل الـ subnets متساويه في العدد

ex.1

57.X.X.X
N | SN=8 | H=16

57.0.X.X 57.1.X.X 57.2.X.X 57.255.X.X

no of subnets = $2^{SN} = 2^8 = 256$ subnets

no of IPs in one subnet = $2^H = 2^{16} = 65536$

ex.2

58.X.X.X
N | SN=16 | H=8

58.0.0.X 58.0.1.X 58.0.2.X 58.0.255.X 58.1.0.X 58.255.255.X

no of subnets = $2^{16} = 65536$ subnets

no of IPs in one subnet = $2^8 = 256$ IP

no of Hosts per subnet = $2^8 - 2 = 254$

* subnet Mask 32-bit Mask 11111---0000
Network part | Host part

ex.1 IP: 63.5.70.120
N | H

Mask: 11111111.00000000.00000000.00000000

255.0.0.0 or /8 ← لو بدل الـ 8 هنا Mask [no of Network bits]

ex.2 IP: 128.50.3.200
N | H

MASK: 11111111.11111111.00000000.00000000

255.255.0.0 or /16

Ex·3

200 . 1 . 1 . X /24

XX XXXXXX

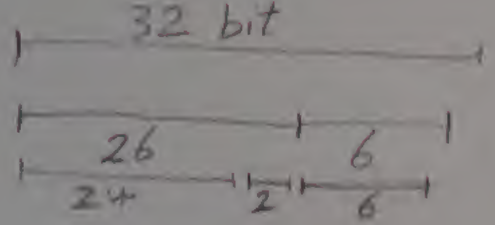
SN H

N

Subnet 1	Subnet 2	Subnet 3	Subnet 4
200.1.1.00000000	200.1.1.01000000	200.1.1.10000000	200.1.1.11000000
200.1.1.00000001	200.1.1.01000001	200.1.1.10000001	200.1.1.11000001
200.1.1.00000010	200.1.1.01000010	200.1.1.10000010	200.1.1.11000010
⋮	⋮	⋮	⋮
200.1.1.00111111	200.1.1.01111111	200.1.1.10111111	200.1.1.11111111
the subnet address	the subnet address	the subnet address	the subnet address
200.1.1.0 /26	200.1.1.64 /26	200.1.1.128 /26	200.1.1.192/26
direct Broad cast address	direct Broad cast address	direct Broad cast address	direct broad cast address
200.1.1.63/26	200.1.1.127 /26	200.1.1.191 /26	200.1.1.255 /26

FATAKA Method

/26



No of subnets $= 2^2 = 4$

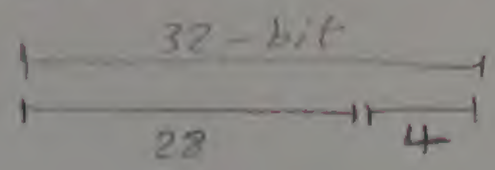
No of IPs /subnet $= 2^6 = 64$ ← the step

	subnet 1	subnet 2	subnet 3	subnet 3
start	200.1.1.0 /26	200.1.1.64/26	200.1.1.128/26	200.1.1.192/26
end	200.1.1.63/26	200.1.1.127/26	200.1.1.191/26	200.1.1.255/26

Ex.1 For the major network 193.168.5.0/24 , Devide it into 16 subnet each contain 16 IP

Sol: No of subnet $= 16 = 2^4$ ∴ New network = 24 + 4 = 28 bit

no of IPs = 16 ∴ New host part = 4 bit



1st subnet address → 193.168.5.0/28 →

2nd ~ ~ → 193.168.5.16 /28

3rd ~ ~ → 193.168.5.32 /28

4th ~ ~ → 193.168.5.48 /28

5th ~ ~ → 193.168.5.64/28

⋮ ⋮

last ~ ~ ~ → 193.168.5.255 /28

Direct Broadcast address

Ex.2 * Find the largest Mask ???

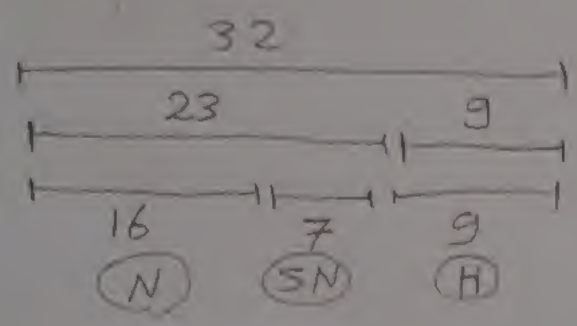
→ /30 ⟨ N = 30
H = 2 ⟹ No of IPs = $2^2 = 4$
No of Hosts = 4 - 2 = 2

PTP او Point to point

كده كده اكبر Network ممكن اعملها من حياتي

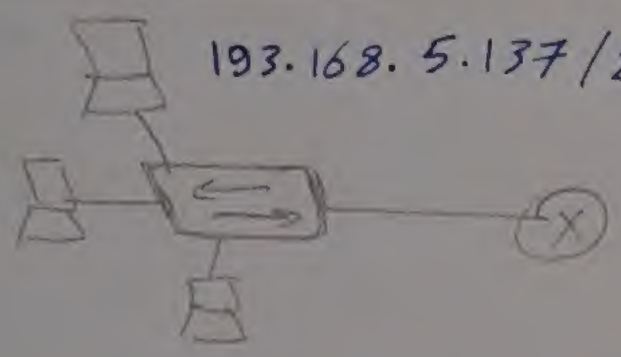
The Mask for this Network = 255.255.255.252 ⟹ ≡ /30
Unes نفس Mask يا

Ex.3 127.16.0.0/16 Devide it to /23



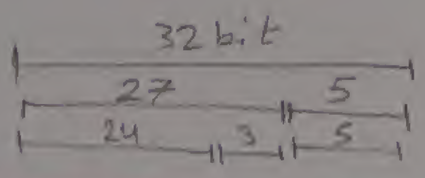
No of subnets = 2^7 = 128
No of IBs = 2^9 = 512
No of Hosts = 510

Ex.4



find
- subnetwork address
- Direct Broadcast address
- valid IPs for Hosts

Sol.
1 FATAKA method



noof subnets = 2^3 = 8
noof IPs = 2^5 = 32 IP
no of Hosts = 30

193.168.5.0/24

193.168.5.0/27 193.168.5.32/27 ---- 193.168.5.128/27 193.168.5.160/32 ----

subnet address ← 193.168.5.137/27

Direct Broad cast address ← 193.168.5.159/27

الطريقة دي ممكن يكون فيها مقدور لو عدد الـ Subnets أكبر أوي

⇒ Solution FATAKA AWY Method

Ip : 193.168.5.137/27

IP : 193.168.5.10001001
N = 27 H = 5

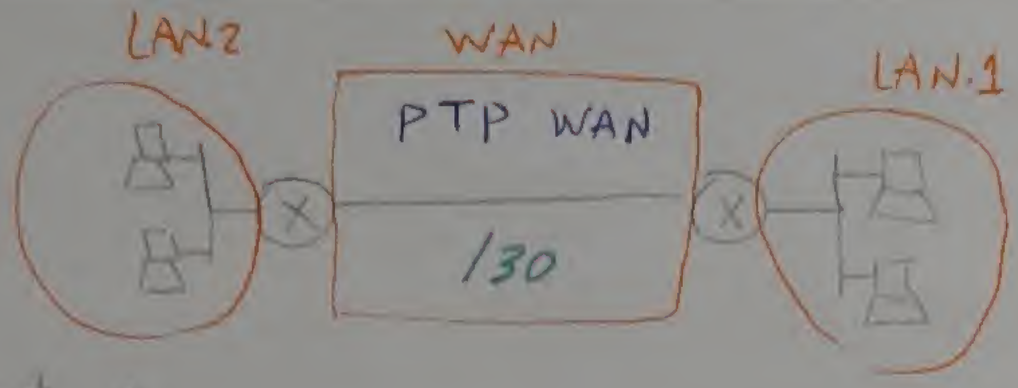
193.168.5.100 00000 = 193.168.5.128 [subnet address]
193.168.5.100 11111 = 193.168.5.159 [direct Broadcast address]

Binary الـ 137 هتطلع ازاي

137
- 128 → 128
9
- 8 → 8
1
- 1 → 1
0

137 = 10001001

IQ technical

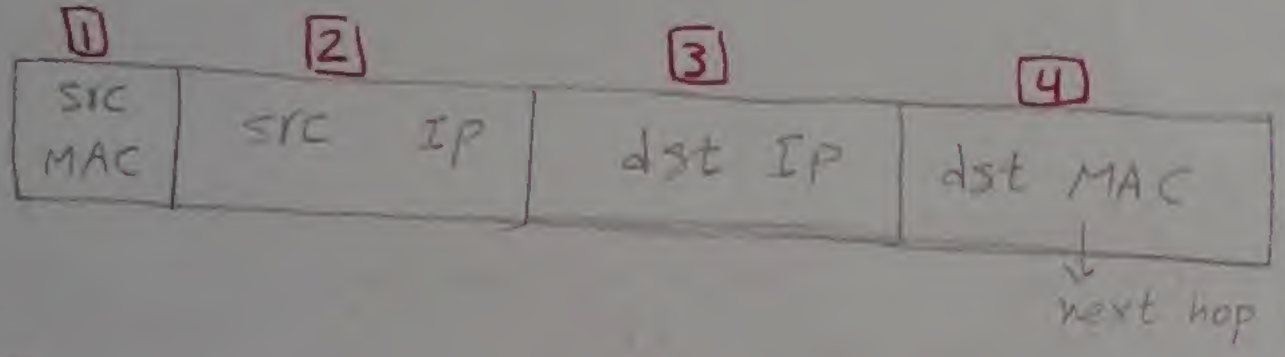


there are 3 networks not 2

---

session 10

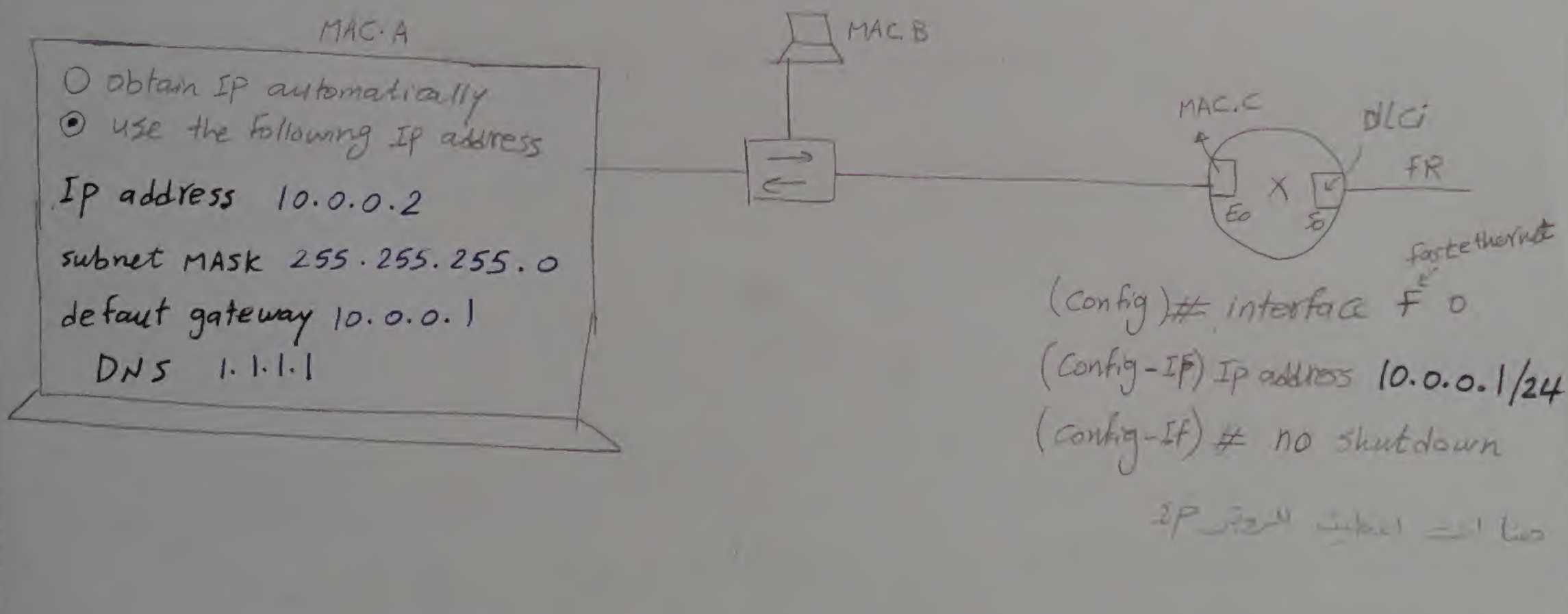
Getting started for end to end data delivery



1 src MAC : it is burnt on Rom of NIC [network interface card]

2 src IP

A manually [you give it to DTEs]



Ip address 10.0.0.2 ①
subnet Mask 255.255.255.0 ②
← الاجهزة دول ال PC يقدر من خلالهم يتكلم LAN فقط

defaultgateway 10.0.0.1 ③ ← الاجهزة ، ال PC يقدر من خلاله يتكلم WAN مع شبكات اخرى

DNS 1.1.1.1 ④ ← من خلال الاجهزة ال PC يقدر يدخل على ال Internet

[B] automatically

servers ... بـ protocol ... من غير ... unicast IP ... ده الـ PC ... ياخد الـ

1 - RARP (old) (revers ARP)

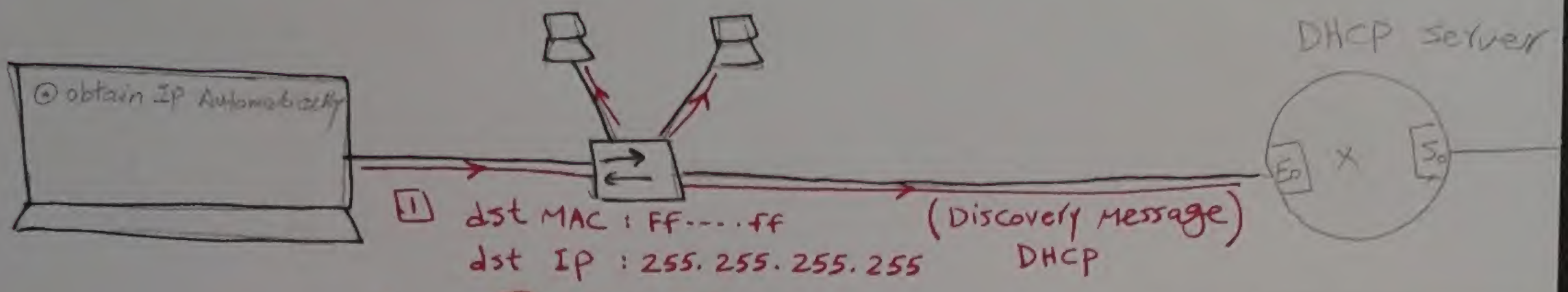
2 - Boot P (old) (Booting protocol)

3 - DHCP (New) (Dynamic Host Configiration protocol)

↳ this protocol exist in layer 7

* اسماء الـ protocols اللي بتستخدم العملية دي

دة اللي بيستخدم حاليا



لو الـ PC موافقه ياخد الـ IP ده ... صيقول للـ server احجزهالي

موافقه

IP DHCP pool

Network : 192.168.1.0 /24

default router : 192.168.1.1 (gateway)

DNS : 4.2.2.2

بعد كتابه الاوامر دي للروتر ← كدة الروتر عرف انه شغال server

pool contains all IPs available in this network

* في بعض الشركات بتعمل 2 servers عشان يخدموا الـ PCs ويوفروا وقت في اعطاء IPs للـ PCs

لو الـ PC بعت رساله للـ 2server و الـ 2server ردوا عليه و الـ PC صيعمل accept على اسرع offer ومش هيقدر يشتغل بالـ IP دة الا لما يجيله ack من الـ server

---

في Interview هيرخم عليك ويقولك ازاي الـ Router يكون L3 ويشغل DHCP اللي هو L7

← بدل ما اشتري server ← انزل اعمل (DHCP) على الروتر وهو هيقوم بدل الـ server و يدي IPs وهنا الروتر عمل وظيفه واحدة بس من L7

وممكن كمان الروتر يعمل Telnet

اثناء تنفيذ الـ ٤ خطوات اللي فاتوا بتظهر الحاجه دي

مرحله بحث

BB الحمد لله لقت والـ PC حصل على IP ← نجاح

⚠ فشل

* the defaut of Automatic Ip is Dynamic , but you can change it to static Ip

Dynamic ← كل ما تقفل الـ PC وتشغله يعطيك Ip مختلف

لو عايز تخليه static Ip تدفع ١٠ جنيه في الشهر كاشتراك الـ Ip

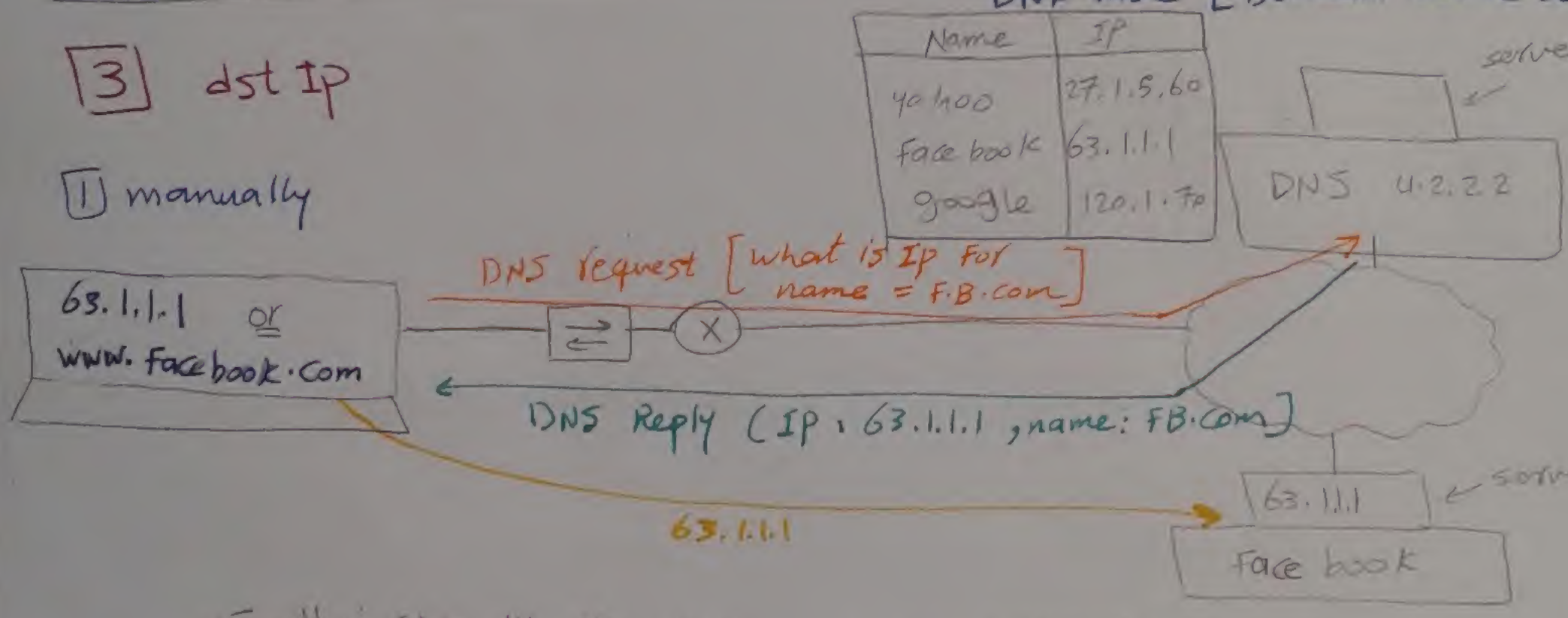
---

3 dst Ip

1 manually

DNS Table [Domain Name server]

Name	IP
yahoo	27.1.5.60
face book	63.1.1.1
google	120.1.Fo



* الـ DNS عبارة عن Internet book زي الـ phone book اللي عندك في البيت

* معندك كتب الـ Ip بتاع الموقع اللي انت عايزه في URL وهو هيوديك لـ server على طول

* او تكتب اسم الموقع www.facebook.com وهنا انت هتبعت request لـ DNS server وهو هيبعت لك الـ Ip بتاع الـ Facebook

* يوجد 13 DNS server حول العالم [٨ منهم في امريكا] وباخدوا الرموز من A ← M

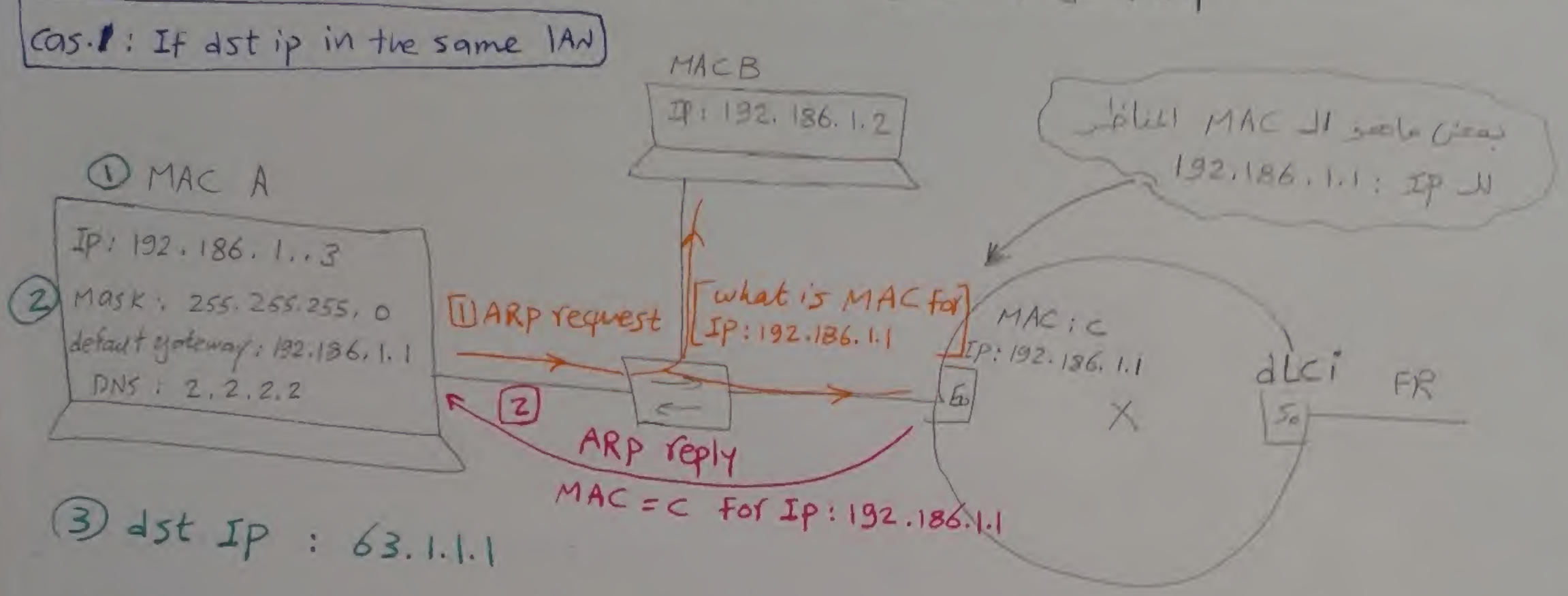
* شركات الـ service provider زي [TE data] بتاخد نسخه من DNS server وتسطبها عندها وانت لما بتعمل request على موقع معين بتروح على الـ server بتاع الـ TE data ويجيبلك الرد ولو الـ server بتاع الـ TE data متعرفش الموقع بقى هيروح على الـ DNS server الاصلي ويعرف منه عليه الـ Ip بتاع الموقع اللي انت عايزه

(3) dst MAC [next hop MAC]

ARP : address resolution protocol

طريقة عمل ال ARP ⇐ بمعلوميه ال dst Ip اقدر اعطيك next hop MAC

cas.1 : If dst ip in the same lAN



③ dst Ip : 63.1.1.1

④ dst MAC ?? (C)

③

ARP Table

IP	MAC
192.186.1.1	C

* ① ال PC هيبعت ARP request ودة نوعه Broadcast
* ② ال Router اللي يعطلك ال Ip (192.186.1.1) هو بس اللي هيرد
* ③ ال PC هياخد الرد دة و هيخزنه في جدول اسمه ARP Table

[اكتب على ال cmd الامر دة ARP -a عشان يعطيك الجدول بتاع ال ARP]

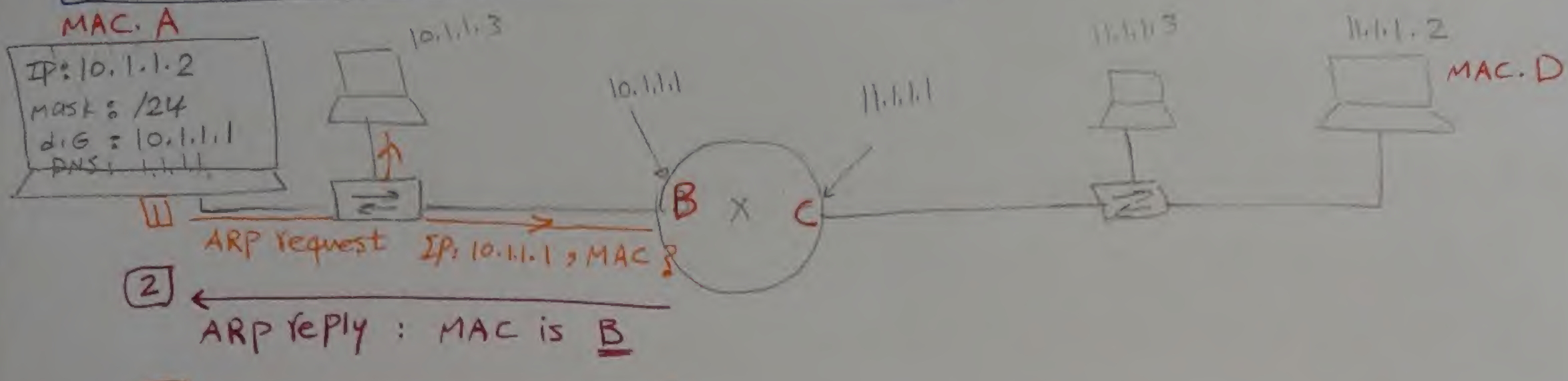
* كل الشرح اللي فوق دة في حالة ال LAN ، نيجي بقى في حالة ال WAN

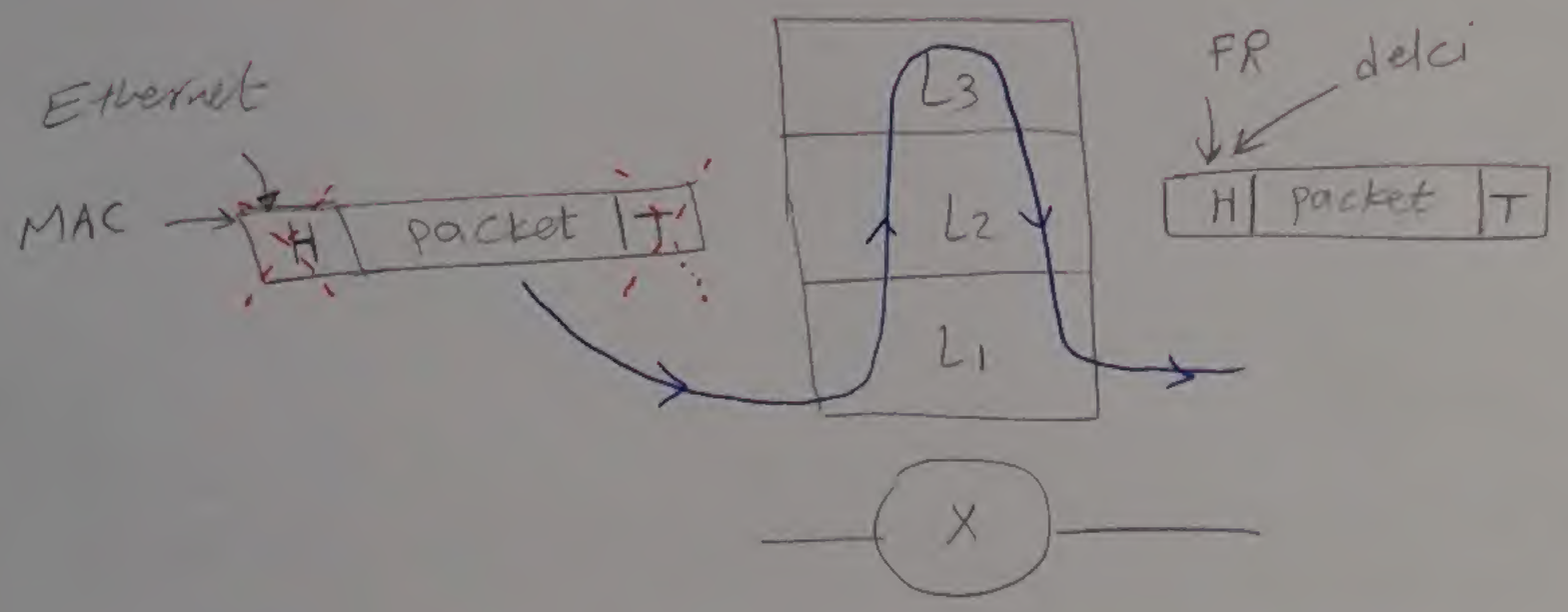
---

* في حالة ال WAN هنفترض بقى انه ال Final end Ip موجودة في LAN تانية

Case 2 : If dst IP in another LAN

Sometimes called proxy ARP





* ملاحظة: الـ dst IP & src IP مستحيل يتغيروا لكنه الي بيتغير هما dst MAC & src MAC

* ملاحظة: الـ ARP بتشتغل في Layer 2

PDU [packet data unit] = segment

layer 4: Transport layer

it is responsible for end to end delivery control

1- segmentation : by deviding data in to smaller parts
2- error detection : by CRC
3- session addressing : by port no. → ؟ ايه هو الـ Application اللي جوا تتكلم على الـ PC اللي انت جوا

port no 16 bit [0 – 65535]

0 — 1023

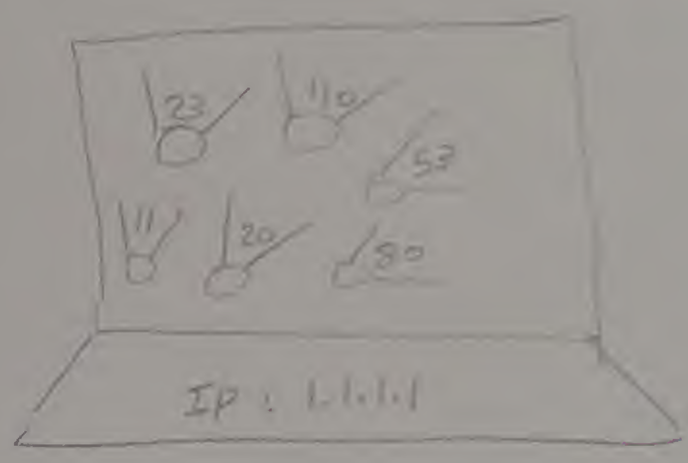
* registered ports [well known ports]
* used by servers

20, 21 → FTP
23 → Telnet
25 → SMTP
110 → POP3
53 → DNS
80 → HTTP
443 → HTTPS ← security

1024 – 65535

* un regulated ports
* session address for users

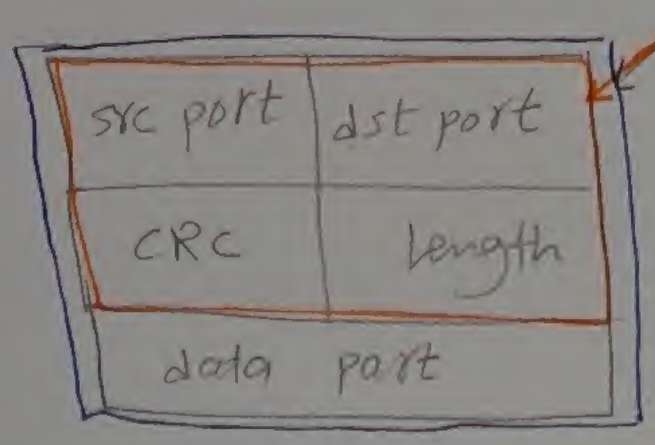
لو انت جاي تعمل server يفضل تعملها هنا

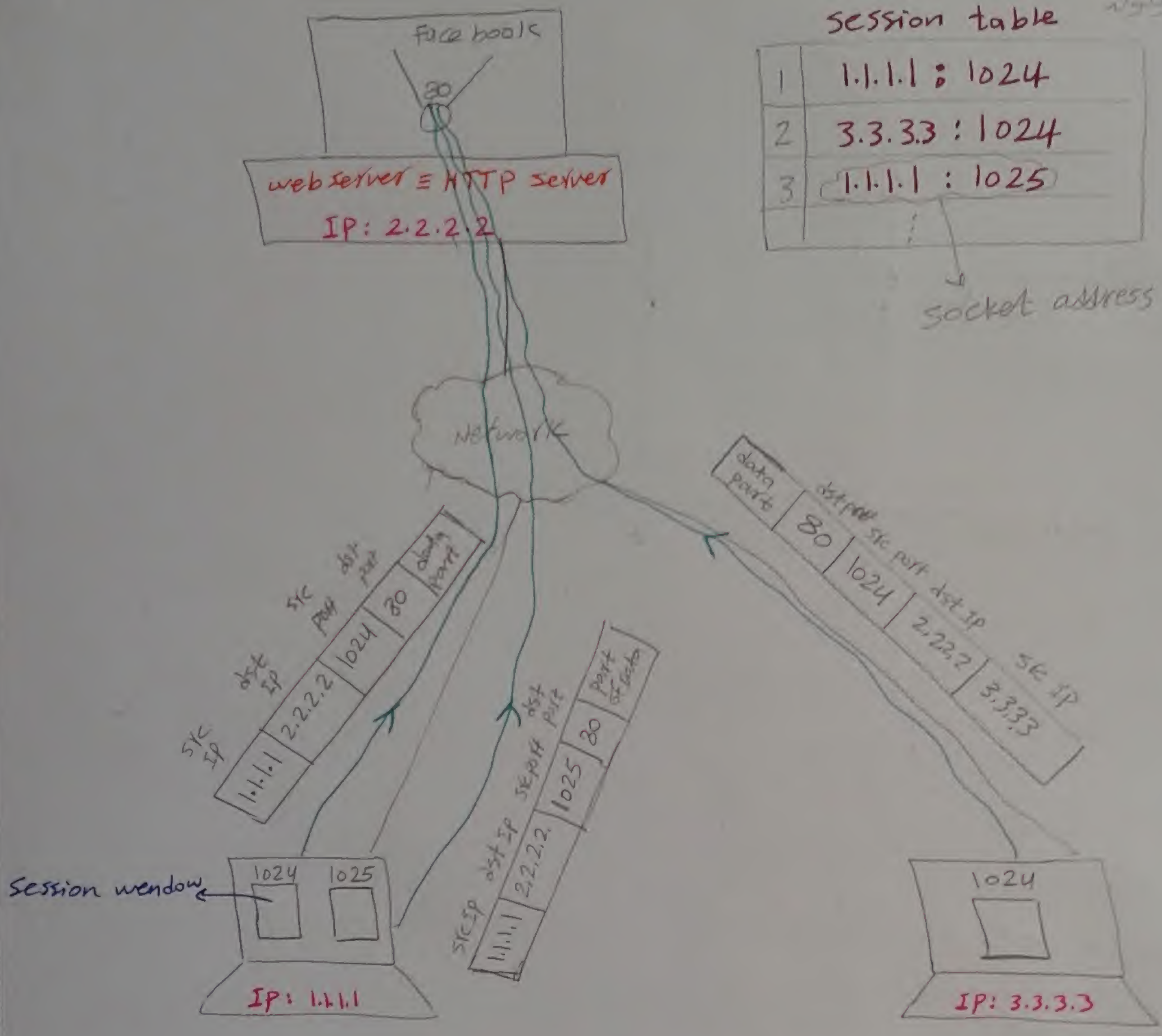


* Socket no = 48 bit or [socket address]

IP : port
32 bit : 16 bit

الـ socket address دي بيعتمد على فكرة التخصيص في IP واحد
زي عندك في البيت انه اكتر من PC كلهم نفس الروتر





---

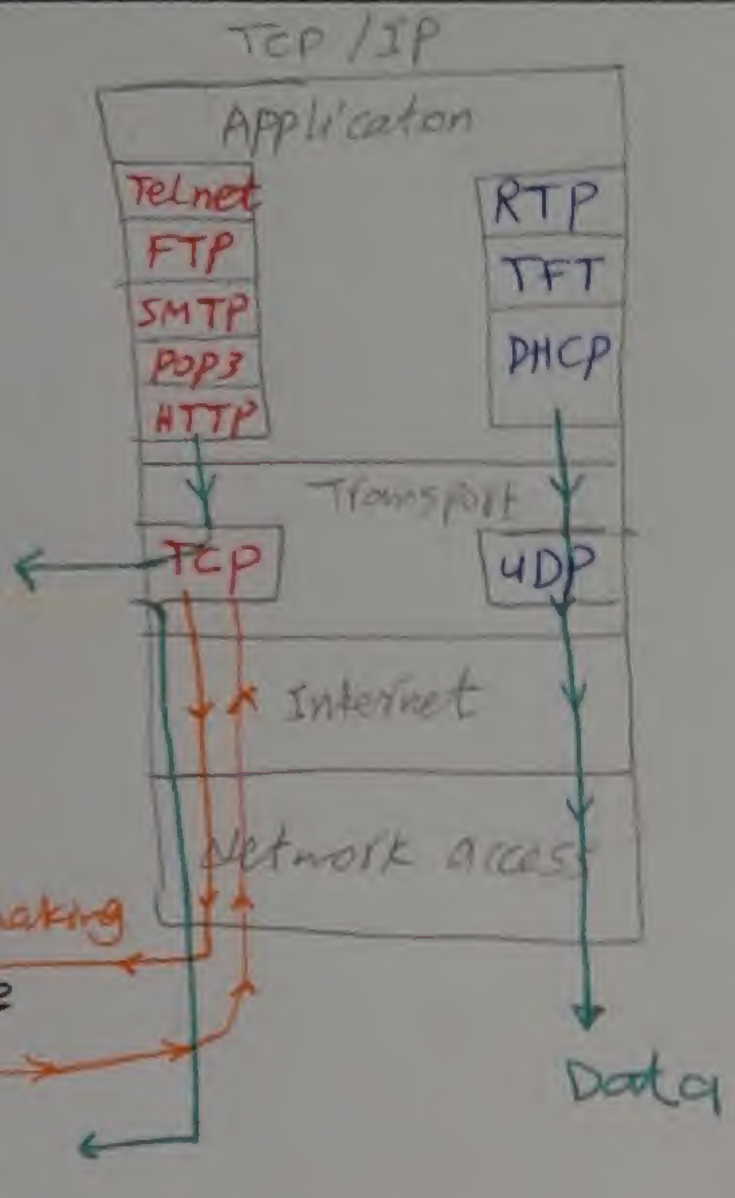
④ Transport layer provide two services

① Connection less service by UDP [User Datagram protocol]

② connection oriented service by TCP [Transmittion control prot]

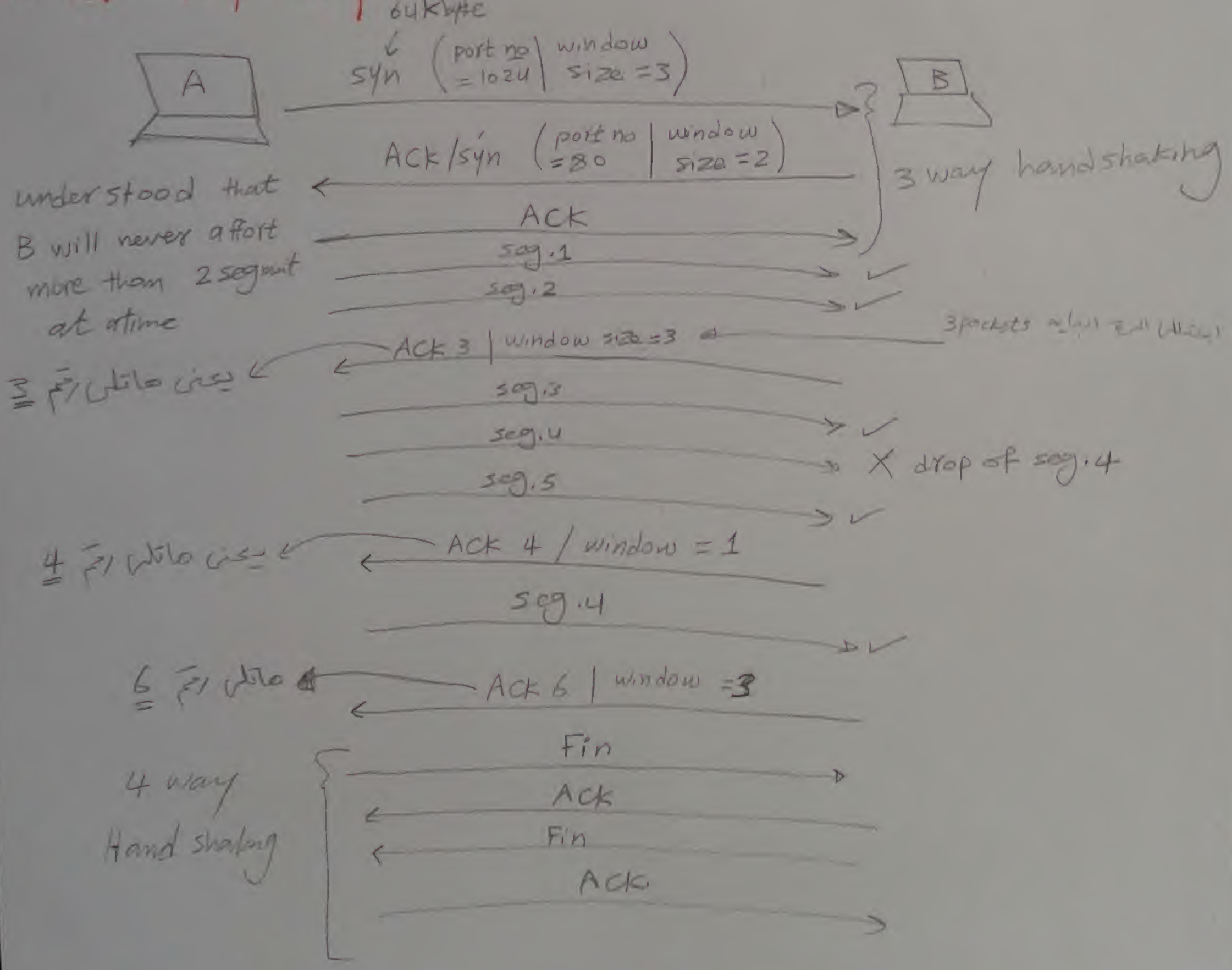
- the services that interest in speed as [RTP] and [TFTP]
  - RTP: Voice, Vedion
  - TFTP ← Trivial Transfere protocol ← عامل زي FTP بس على اجام صغيرة
- * بمعنى انه UDP مش شرط يتأكد انه الداتا توصل لل dst ولا لأ
  يعني انه يفرجها في الحال

Telnet, FTP, SMTP, POP3, HTTP زي Application اللي محتاجه دقه ← لو حد ك
بمعنى انه لما تيجي داتا بيجزها عندة وبيبعت Handshaking msg يتأكد هل الداتا توصل ولا لأ


TCP /IP
Application
Telnet
FTP
SMTP
POP3
HTTP
RTP
TFT
DHCP
Transport
TCP
UDP
Internet
Network access
Data
Data
end device
Handshaking
parking of data
untill hand shaking
operation will be
success
1
2

---

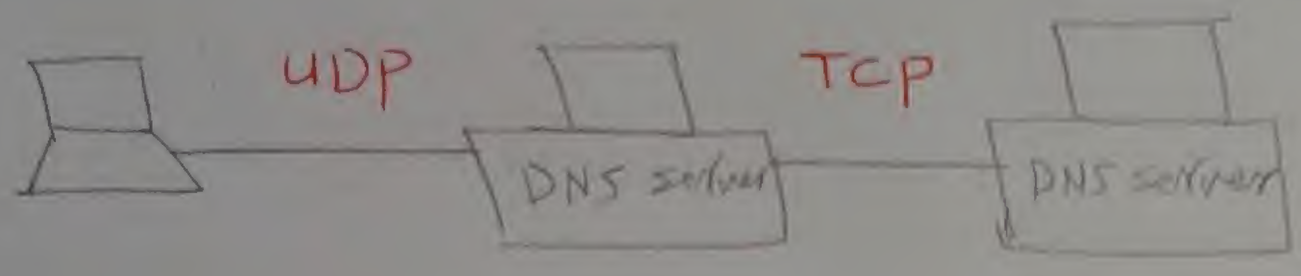
* For TCP only


A
B
64Kbyte
syn (port no =1024 | window size =3)
Ack/syn (port no =80 | window size =2)
Ack
3 way handshaking
understood that
B will never affort
more than 2 segment
at atime
seg.1
seg.2
Ack 3 | window size =3
3 packets
seg.3
seg.4
seg.5
X drop of seg.4
Ack 4 / window = 1
seg.4
Ack 6 | window =3
Fin
Ack
Fin
Ack
4 way
Hand shaking

Interview question

س : الـ DNS بيشتغل مع TCP ولا UDP

جـ : الاتنين



Note in subnets :-

* old subnetting standard : while subnetting , don't use first and last subnets
→ leave them for future → no of subnets = $2^{SN} - 2$

* new subnetting standard : you can use all subnets

Routing Introduction

* Routed protocol : it is used to carry user data triffic from end to end
مُوَجَّه ← مُوَجَّه - مُتَوَجَّه ← مفعول به

by - encapsulating data end to end
- supporting logical addressing

ex: IPV4 - IPV6 - IPX - AppleTalk

* Routing protocol : it is the exchange of information between Routers
فاعل ← مُوَجِّه
, so as each Router tell the other about networks it can reach

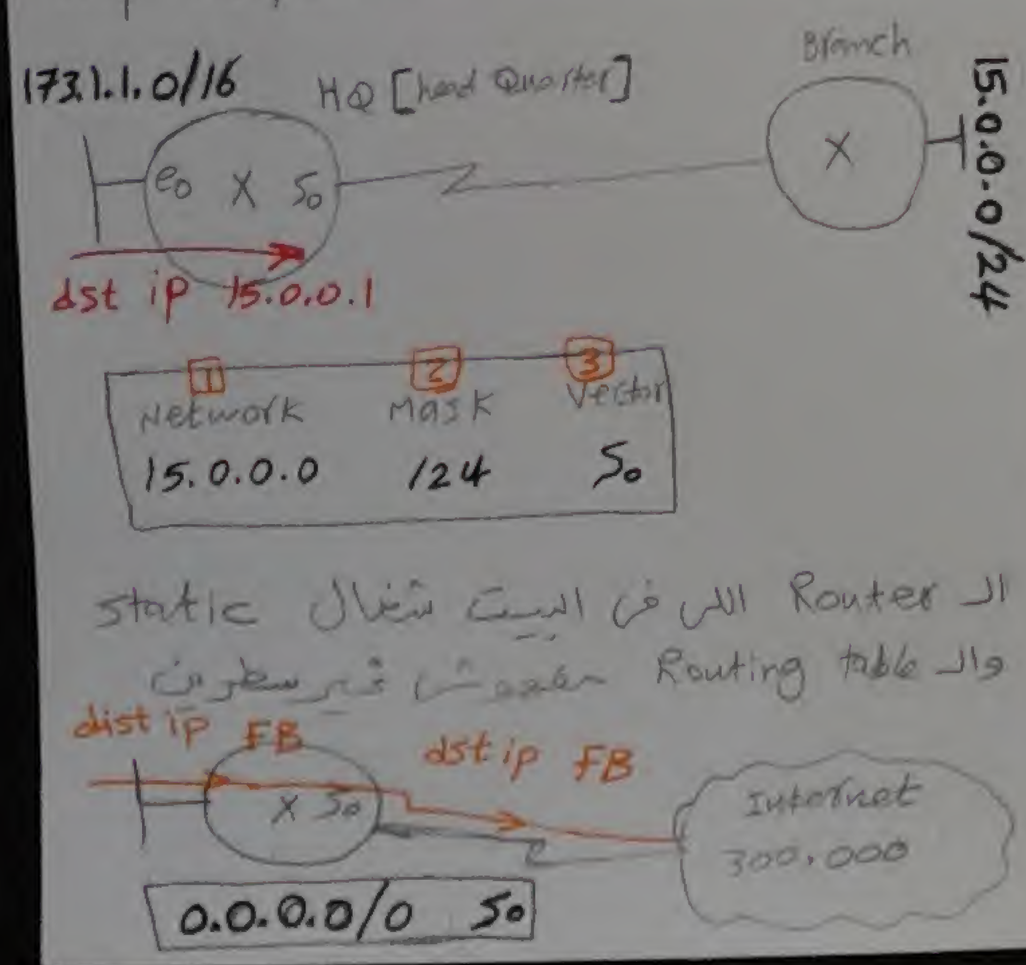
its final target is to build Routing table [Network MAP]

ex: distance vector: RIPV1, IGRP, RIPV2, EIGRP (افضل واحد) — Advanced distance vector — By Cisco
link state: OSPF, ISIS
BGP (بتاخد من CCIE)

Routing classification

Static Routing

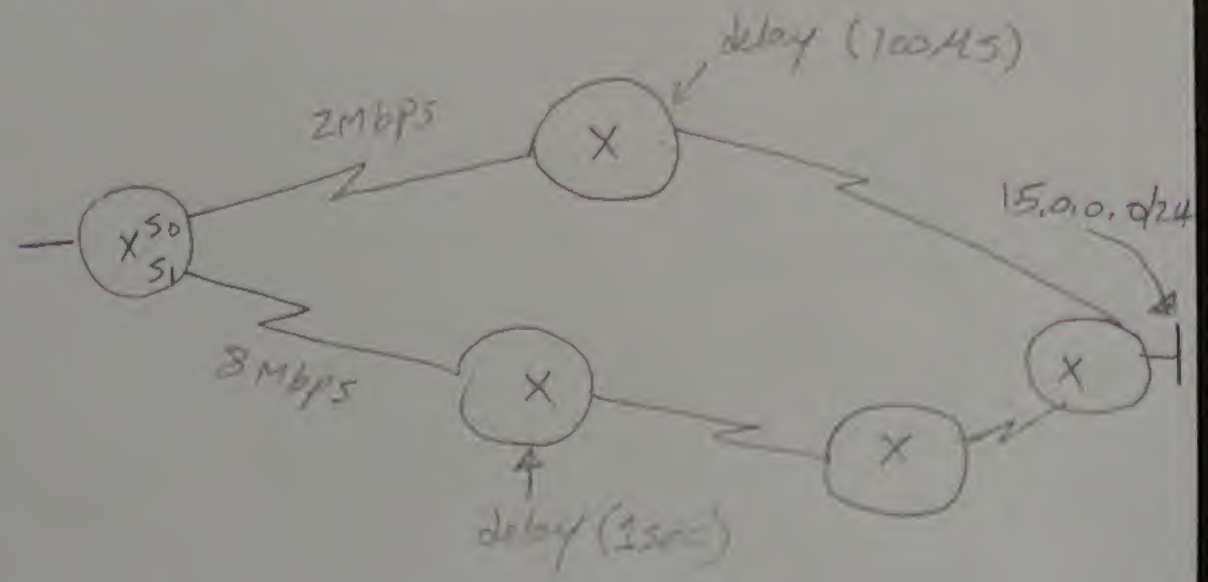
* building the routing table manually
* used for simple Networks
only one path exist to dst network



static اللى فى البيت شغال الـ Router والـ Routing table معمولش غير سطرين

Dynamic Routing

* Building routing table automatically by s/w called routing protocol
* used If Network is complex
more than one path exist to dst



Dynamic Routing

IGP [interior Gateway protocol]

"routing protocols that work inside Autonomous system"

ex
- Distance vector (D.V) [RIPv1 & IGRP]
- advanced D.V [RIPv2 & EIGRP]
- Link state [OSPF & ISIS]

EGP [exterior Gateway protocol]

"routing protocols that work between Autonomous systems"

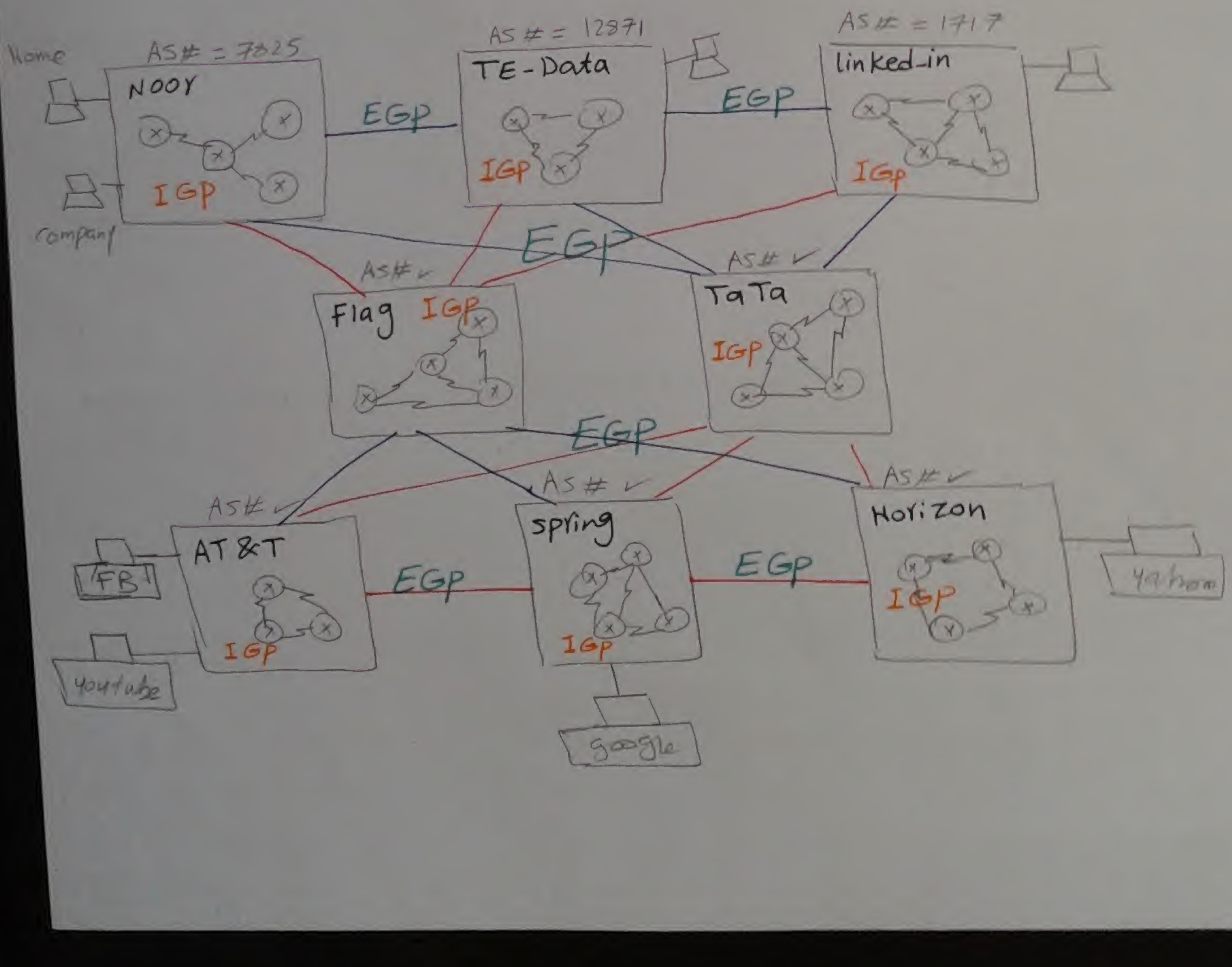
ex: EGP [old]
BGP [New] [Boarded Gateway protocol]

وده عباره عن Translator بين الـ Autonomous systems (يعني)

Automomous system : نظام مستقل

it is a group of devices that is under single Technical Administration or under single routing policy

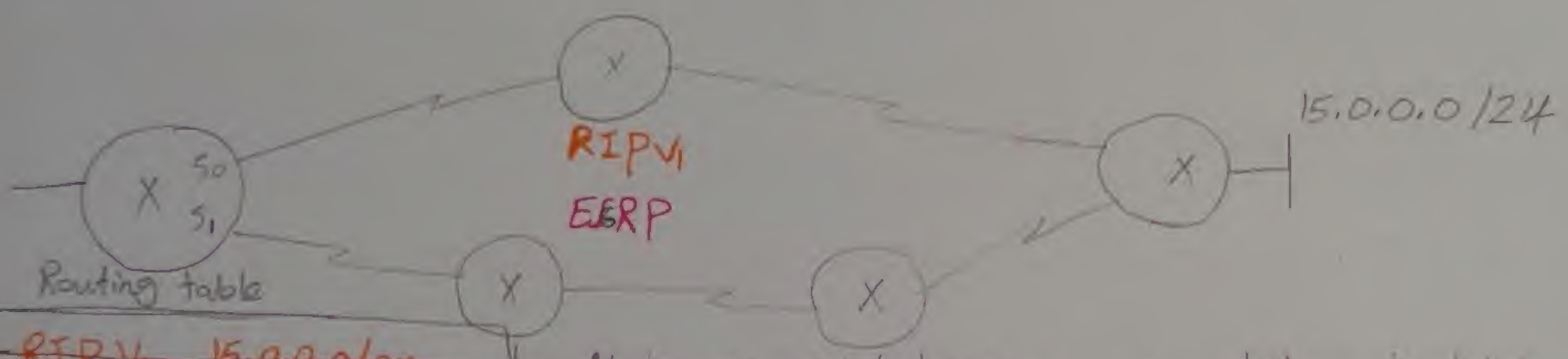
Autonomous sys (AS) number → [0 → 65535]



* Routing table :- it contains :-
  - the best protocol [If many exists]] → it has the best of the best
  - the best path [If many exists]]

* the best protocol is protocol that having least administrative distance

admin. distance / it is a number from [0 - 255], each routing protocol has a unique no, that number reflect thruthfullness [preference] of protocol



→ It is canceled because admin distance is high 120

لو في طريقين في نفس الـ protocol يوصلوك لـ Network معينه ⇐ الـ Router هيختار افضل طريقه ودة بيعتمد على الـ Metric (المسافة) [الاقل مسافه هو اللي هيكمل فيه وهيحزف الطريقه التاني] ☺

The best path is having the least Metric ≡ cost مسافه

IETF : internet Engineering ← اسم الهيئه اللي بتحط الـ admin. distance

protocol	admin. distance
RIPv1, V2	120
ISIS	115
ospf	110
IGPR	100
EIGPR	90
BGP	20
static	0, 1

The best the protocol, the least the admin. distance

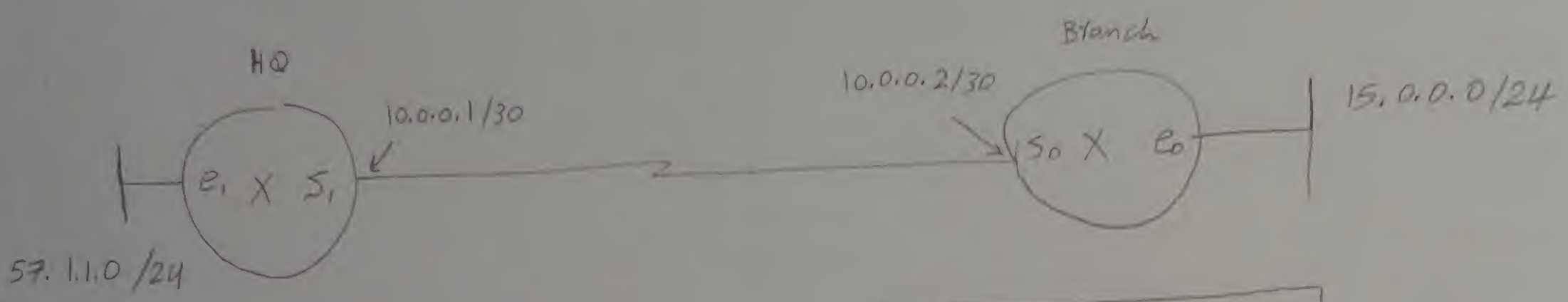
metric ≃ cost

- hop count — no of routers — ex: RIP V1, V2
- Band width (speed) — Metric ∝ 1/BW
- delay (late)
- load (congestion) الحمل
- reliability (stability)
- MTU [Maxi. Transfere unit] — packet الـ

* Static Routing

[1] Connected Networks ⟶ (C)
[2] Static Route ⟶ (S)
[3] Static to all ⟶ (S*)

← Routing table الروتر في ال



Connected → C 57.1.1.0/24 e1
C 10.0.0.1/30 S1
static ← S 15.0.0.0/24 S1

C 15.0.0.0/24 e0
C 10.0.0.2/30 S0
Static to all ← S* 0.0.0.0/0 S0

(Config) # ip route Network Mask { name of exit interface | or - IP of next hop - - - - Router - - - - gateway }

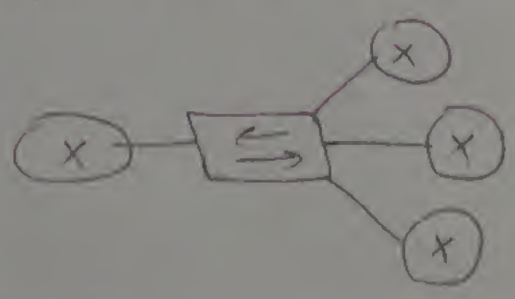
[1] [2] [3] Vector

* HQ (Config) # Ip route 15.0.0.0 255.255.255.0 S1 → admin distance = 0

point to point topology في حالة S1 الي في حالتنا interface انت بتكتب اسم ال فقط

* HQ (Config) # Ip route 15.0.0.0 255.255.255.0 10.0.0.2/30 → admin distance = 1

انت بتكتب اسم ال Vector [10.0.0.2/30] في حالة لما تكون الشبكة star topology يعني
point to Multipoint



Brand (Config) # ip route 0.0.0.0 (Network) 0.0.0.0 (Mask) S0 (vector)
[1] [2] [3]

+ (Config) # IP Classless

The First 1.15 hr is Lab

Routing classification

- Static Routing
- Dynamic Routing
  - IGP
    - Distance vector
      - RIP V_1
      - IGRP
    - Advanced D.V
      - RIP V_2
      - EIGRP
    - link state
      - ospf
      - ISIS
  - EGP
    ex: EGP , BGP

---

* Distance vector (D.V.)

ex: - RIP V_1 : Routing information protocol V_1
- IGRP : interior Gateway Routing protocol [by cisco]

* D.V. operation

① at start up = just after configuration
② at convergence = steady state
③ at change = If new network appears or network disappears

* في ال D.V protocol بيحسب ال Metric عن طريق عدد ال hops

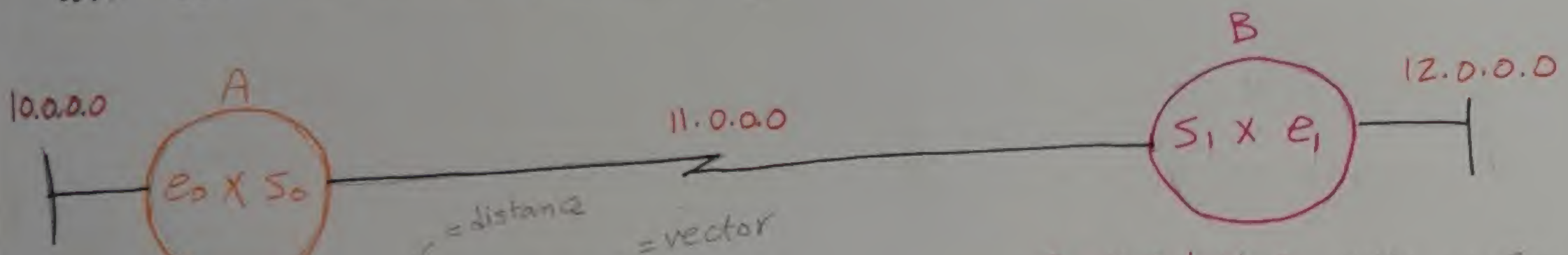
* each 30 sec , each router will send its Routing table in IP packet whose IP = 255.255.255.255

* this IP is the Direct Broadcast IP that force all Routers connected to our Router to process the packet that includes the Routing table

* note , the Router can send Broadcast msg . but It doesn't route the incoming Broadcast message

يعني انه الروتر ينفع يرسل Broadcast لكن لو جاله Broadcast مش صيغديو وصياخدها لنفسه

[1] at start up :
each Router will take a copy of all Routing table entries, add (1 me) to the metric & send the modified entries out of all its interfaces periodically



Routing table·A

		metric	interface
C	10.0.0.0	0	e_0
C	11.0.0.0	0	S_0

(connected)

Routing table·B

		metric	interface
C	12.0.0.0	0	e_1
C	11.0.0.0	0	S_1

* After 1st periodic update (30 sec)

Routing update [Routing advertisement] (Packet) →
11.0.0.0 , (1) → you can reach This Network by one hop
10.0.0.0 , (1) → who is me
as above

←
12.0.0.0 , 1
11.0.0.0 , 1

admin. distance ⟹ represent how metric is.

ملحوظه / كل Router هيعمل الـ update بعد 30 ثانيه من ساعته الخاصه يعني مش شرط الاثنين يعملوا update من نفس اللحظه

	C	10.0.0.0	0	e_0
0 =	C	11.0.0.0	0	S_0
120 =	~~R~~	~~11.0.0.0~~	~~1~~	~~S_0~~
	R	12.0.0.0	1	S_0

RIP

هنا الروتر وجد عنده الـ Network 11.0.0.0 متسجله عنده هوتين ← هيشوف الـ admin distance بتاع كل سطر وهيعرف السطر اللي فيه الـ admin distance قالل

C	12.0.0.0	0	e_1
C	11.0.0.0	0	S_1
~~R~~	~~11.0.0.0~~	~~1~~	~~S_1~~
R	10.0.0.0	1	S_1

* After 2nd periodic update

←
10.0.0.0 , 1
11.0.0.0 , 1
12.0.0.0 , 2

→
12.0.0.0 , 1
11.0.0.0 , 1
10.0.0.0 , 2

	C	10.0.0.0	0	e_0
	C	11.0.0.0	0	S_0
	R	12.0.0.0	1	S_0
still alive ←	R	12.0.0.0	1	S_0
	~~R~~	~~11.0.0.0~~	~~1~~	~~S_0~~
	~~R~~	~~10.0.0.0~~	~~2~~	~~S_0~~

لو الـ Router وجد انه فى سطرين ليهم نفس الـ Network ونفس الـ admin distance ⟸ هيشوف still alive دى الـ Network انه الـ

C	12.0.0.0	0	e_1
C	11.0.0.0	0	S_1
R	10.0.0.0	1	S_1
R	10.0.0.0	1	S_1 → still alive
~~R~~	~~11.0.0.0~~	~~1~~	~~S_1~~
~~R~~	~~12.0.0.0~~	~~2~~	~~S_1~~

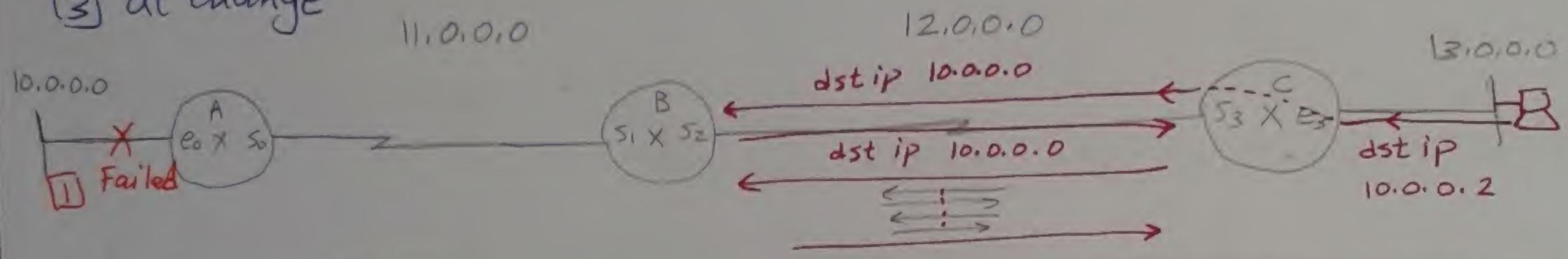
[2] at convergence [steady state]
although convergance, there is still periodic upade to be sure that Networks are still alive

* عشان يعرف الشبكه وقعت ولا لأ ⇐ invalide timer هيعمل ⇐ يعني لو شبكه وقعت الروتر هياخد القرار انه يحذفها من الجدول بتاعه لكن قبل ما ياخد القرار ده هيعمل انتظر عليها يمكن هي مارالتي موجودة لكن في مشكلة بسيطه حصلت

Invalid timer = 6 * updates = 6 * 30 sec = 180 sec = 3 min.

---

[3] at change



[2] After 30sec

~~C~~	~~10.0.0.0~~	~~0~~	~~e0~~
C	11.0.0.0	0	s0
R	12.0.0.0	1	s0
R	13.0.0.0	2	s0

[3] after 30 sec →
10.0.0.0 ,16 = ∞ [unreachable]
11.0.0.0 ,1
12.0.0.0 ,2
13.0.0.0 ,3

C	11.0.0.0	0	s1
C	12.0.0.0	0	s2
[4] R	~~10.0.0.0~~	~~1~~	~~s1~~
R	13.0.0.0	1	s2
[4] R	10.0.0.0	3	s2

[5] after 2nd 30 sec →
11.0.0.0 ,1
12.0.0.0 ,1
13.0.0.0 ,1
10.0.0.0 ,16

C	12.0.0.0	0	s3
C	13.0.0.0	0	e3
R	11.0.0.0	1	s3
R	10.0.0.0	2	s3

[4] ←
13.0.0.0 ,1
12.0.0.0 ,1
11.0.0.0 ,2
10.0.0.0 ,3
⇐ هيضيف السطر ده في Router B بتاع Routing table

there are two problems :-

[1] slow convergence
في حاله ان 10.0.0.0 وقعت * اولا RouterA هيعرف فالحال . ثانيا من RouterB هيعرف ان 10.0.0.0 وقعت الا بعد 30 sec عند طريقه RouterA وكمان RouterC هيعرف الا بعد 30 sec عند طريقه RouterB ← يبقى RouterC عرف بعد 60 sec

[2] L3 Routing loops → التوضيح في الرسمه فوق

[1] الشبكه 10.0.0.0 وقعت
[2] RouterA هيحذفها من الجدول بتاعه وهيبعت [3] لـ RouterB * معلومه تفيد
ذلك بالاضافة 10.0.0.0 ,16 وهنا معنى ∞ = 16 والرقم 16 تم حسابه على اساس ان اقوى Autonomus system في الوقت ده لا تزيد عدد الـ Hops فيه عن 16 hop [لا يمكن الروتر يتم 16 hop ولا بعض في نفس AS وكمان بروتوكول الـ RIP بيستخدم في الشبكات الصغيرة]

4 Router B هيحذف الـ Network عنده مع 10.0.0.0

5 بعد 30 sec و Router B هيبعت update لـ Router C بأن 10.0.0.0 مش موجودة بنفس الامر اللى فات

← كده صلاح المشكله من خطوة 4 ودى حاله الـ 30 sec بتاع الـ update بتاع Router B و Router C وصل وارسله الى Router B • فى الحاله دى Router C هيرسل 3 و 10.0.0.0

* صنابقى لازمه فى الـ Router B هيقارن المعلومه اللى وصلتله من Router A [16و10.0.0.0] و المعلومه اللى لسه واصله من Router C [3و10.0.0.0] و هيضطر انه يحذف سطر من الاتنين ← فهيحذف الطريقه الاسوأ [16و10.0.0.0]

* صنابقى لو جه PC ذات IP = [13.0.0.2] وعايز يكلم حد من Network 10.0.0.0 ⇐ Router C هيقول لـ packet اله

الطريقه لازم تروح له ناحيه Router B عشان هو جايب اسم الـ Network 10.0.0.0 منه و لما تروح الـ packet لـ Router B هيقولها اذهبى الى Router C عشان انا اعرف الـ Network 10.0.0.0 من طريقه

و هتفضل الـ packet تلف حولين الروترين B&C

⇐ المشكله الاساسيه هنا ان العمليه دى هتشغل الروترات جداً

وكده الحل فى ↓

1 TTL [Time to live] expired

بيساوى الـ TTL دة [256 مرة] كل ما الـ packet تعمل Hop ينقص من الـ TTL واحد لحد ما يبقى خانه الـ TTL فى الـ packet = 1 و اول ما الروتر يشوفها بـ 1 هيحذف منه 1 و هيعمل لـ packet ⇐ drop

لأنه مانا هتشغل الروترات 256 مرة [كتيييير]

[2] Triggered update + poisoned Route + poison reverse

حل مشكلة الـ slow convergence بنسبه ٪100
~ ~ ~ ~ Routing loop بنسبه ٪95

[1] اول ما 10.0.0.0 تقع من Router A [5] حيتبعت لبيه وحيتشاله من الجدول بتاعه Routing table الـ [Immediatly] حيبعت من الحال Router A

[3] لـ Router B وحتى حيستنى الـ 30sec بتاع الـ Routing update

[4] Router B حيتشاله من الـ Routing table بتاعه

[5] Router B حيبعت رسالتين . الاولى (Ack) لـ Router A عشان يقوله الـ update وصل و التانيه حيبعت فى الحال [Imm.] الـ Routing table بتاعه لـ Routerc

لكن المشكله زى المره الاولى لو تم خطوة [4] و Routerc بعت الـ Routing table بتاعه قبل Router B بنص ثانيه

⇦ كده احنا وقعنا فى نفس المشكله بس قلنا نشبه الـ error اوى

الرسمه اهى

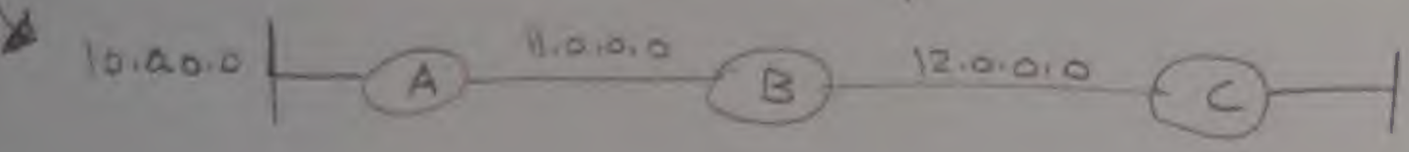
(3) split horizon (الأفق البعيد) : route that learnt from an interface should never be advertized back on the same interface

الحاجه اللي الـ Router اتعلمها من Interface معين - ميتفعش يعلّمها له Interface اتاني على نفس الـ Router

[اللي علمني حاجه ، ميتفعش اعلمها له تاني]

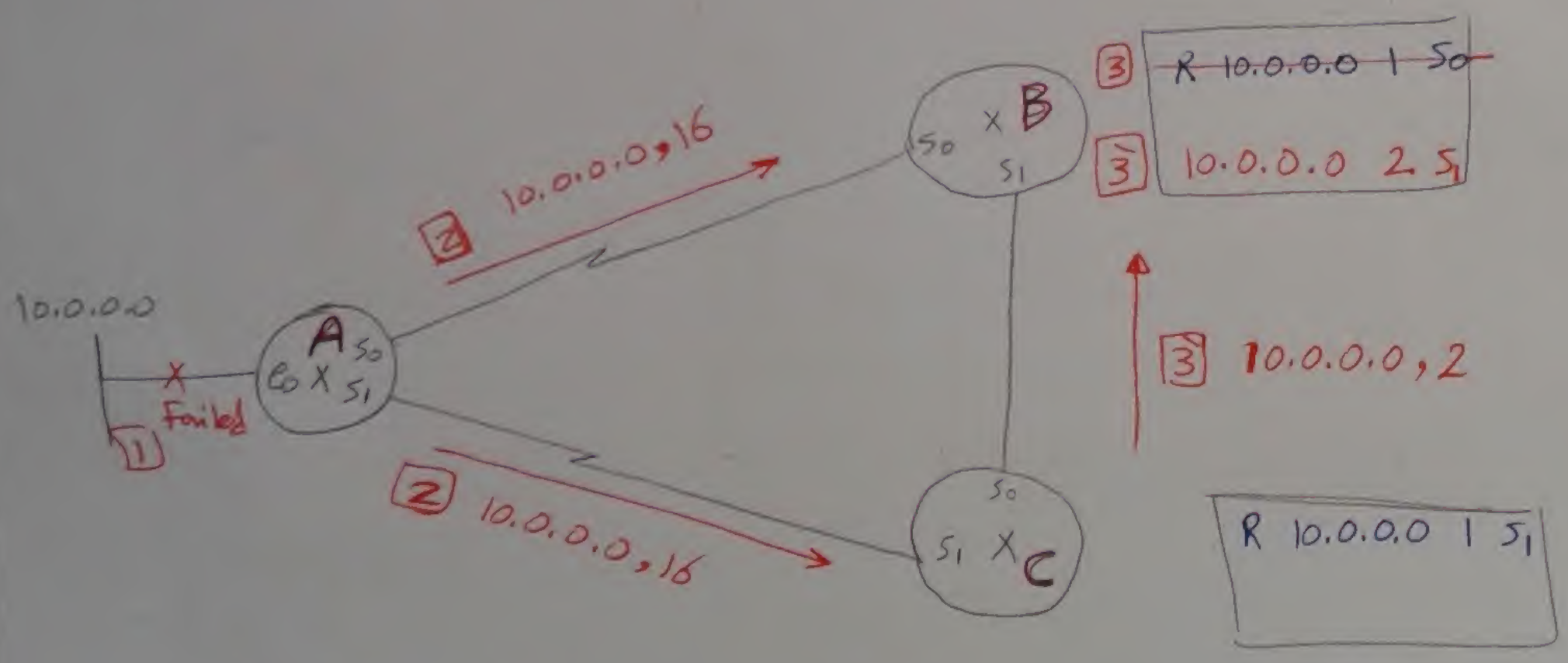
← يعني ايه Router C اتعلم او اتعرف على 10.0.0.0 عن طريق Router B ، عشان كده Router C ميتفعش يقول لـ Router B اي معلومه عن الـ Network 10.0.0.0

وبكده انا حليت مشكله الـ loop في الرسمه اللي فاتت



ولكنه تبقى المشكله في حاله ان Router C يعرف طريقه تاني يوصل عن خلاله لـ 10.0.0.0

← هنا بقى Router C يقدر يقول لـ Router B على اسكه التانيه ويحصل Routing Loop تاني كما تري في الشكل اتضح



وكانه الحل التنين في الطريقه الجاهزه [طريقه الصبي]

(4) Hold down timer (طريقة الهبل)

← حلت مشكلة الـ loop بس 100٪ على حساب الـ convergence

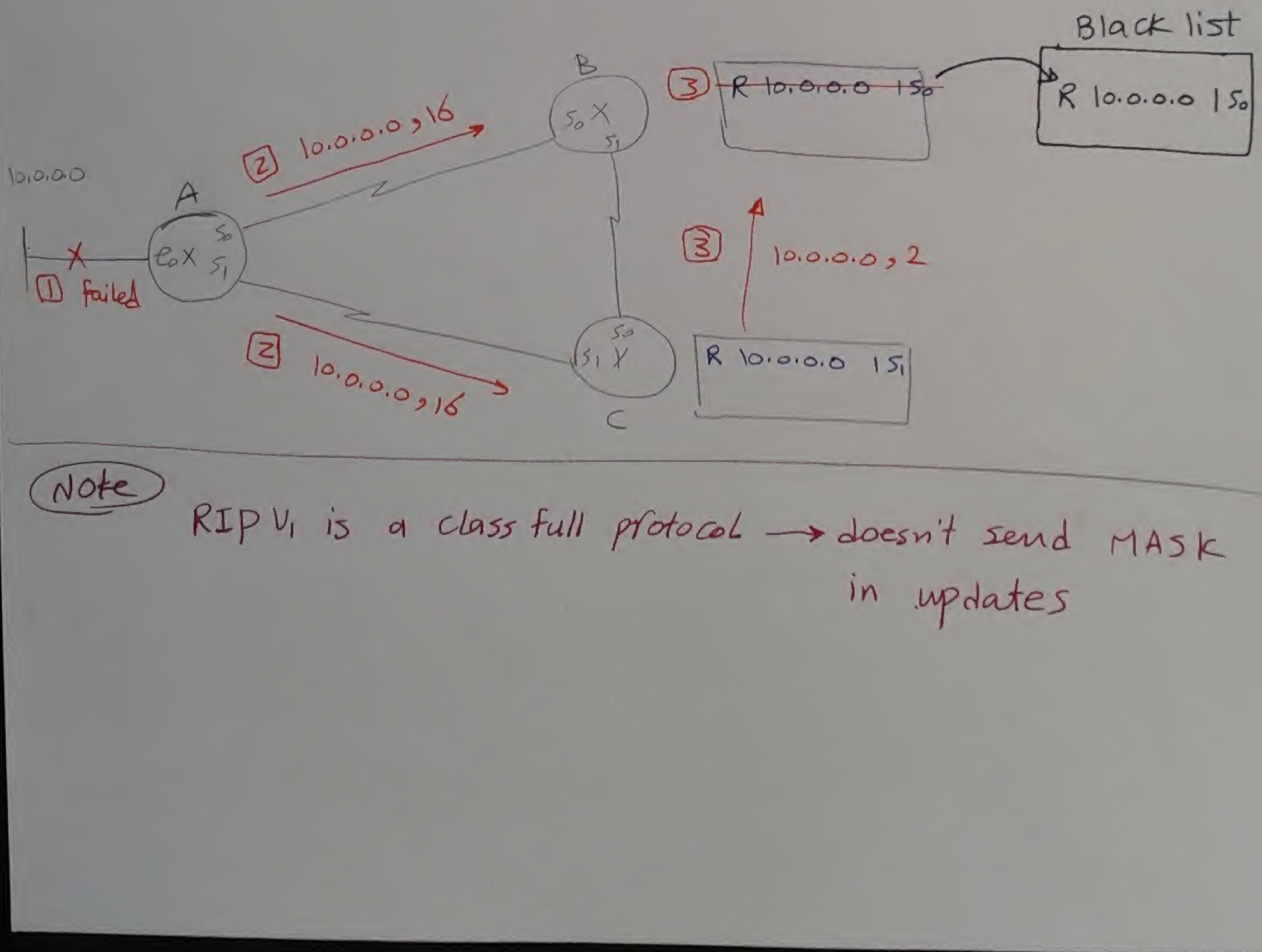
If route failed, donot accept any update about that loop

unless → (1) it returns back back [يعني لو جت بنفس الاتجاه و المسافة]

→ (2) Hold down time expires [180 sec]

← يعني / لو مر 180sec و الروتر الاخر مازال مصمم ان الـ network موجودة الروتر بتاعنا هيفضل يبعت له و يعمل update

الحاجه الزيادة هنا ان Router B هيعمل table جديد Black list اسمه (10.0.0.0) وهيضع فى الـ Black list الشبكة اللى وقعت ولو اتى له اى update بالشبكه (10.0.0.0) هيلاقيها كتبة فى الـ Black list ← ومش هيقبل الـ update الا فى الحالتين اللى فوق (مشروحه)

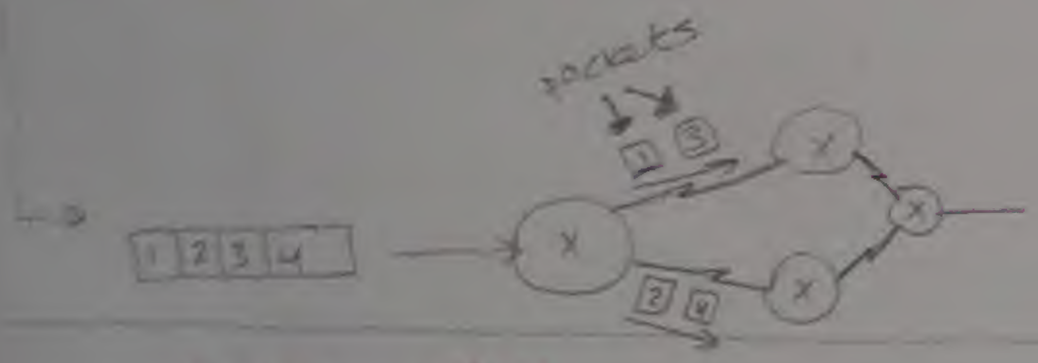


Note

RIP V1 is a class full protocol → doesn't send MASK in updates

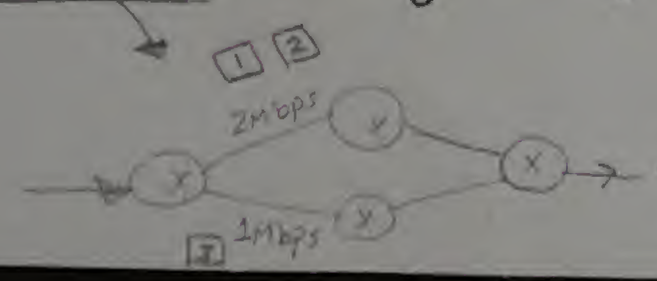
RIPv1 C/C's

1- it is Distance vector D.V Standard routing protocol
2- send periodic update every 30 sec out of all interfaces on Broadcast address 255.255.255.255
3- use A- Triggered update + poisoned route + poisoned reverse
B- split Horizon
C- Hold down time (180sec)
4- symbole in Routing table "R"
5- admin. distance = 120
6- metric = hop [max = 15 hop & 16 = ∞]
7- use Bellman ford Algorithm to calculate the best path
8- support Equal load sharing [load balancing] → defaut 4 paths
max → up to 16 or more
9- class full protocol [doesn't send MASK in update]
The Router that receives the update will estimate the mask



IGRP C/C's

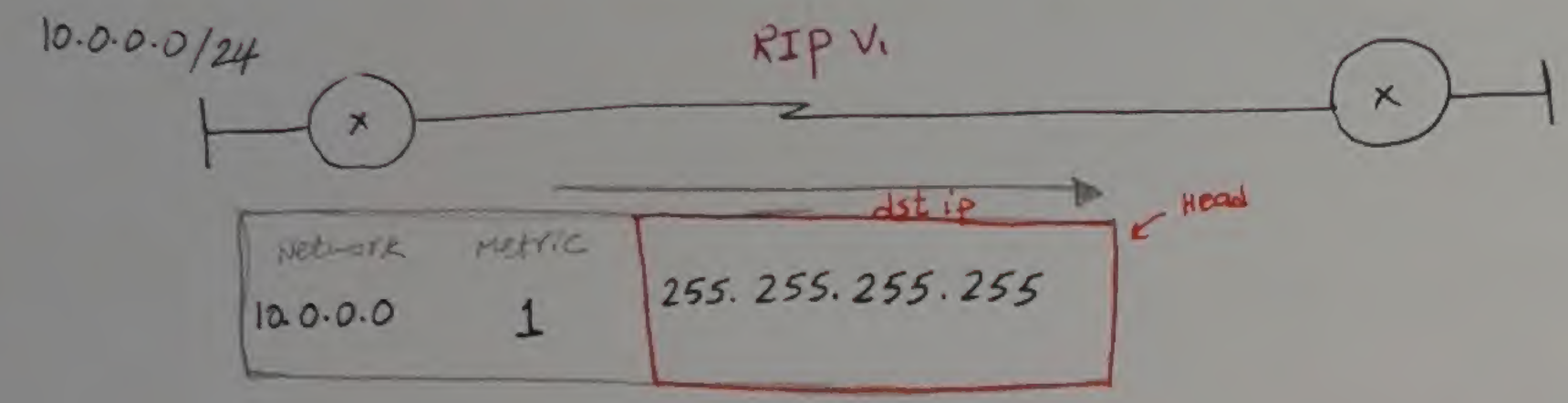
1- it is D.V. Cisco proprietary Routing protocol
2- send -- -- 90 sec -- . 255.255.255.255
→ is more better because it يوفر the processor & memory
3- use A — — —
B ———
C — —— . (280 sec)
4- "I"
5- 100
6- metric is composite { B.W , delay , load , reliability , MTU } (default)
7- ———
8- support Equal & unEqual loading sharing [4 default, 60 or more]
9- Classfull



2packet ← 2
1packet ← 1

ADVanced Distance vector :- ex: ① - RIP v2
③ - EIGRP

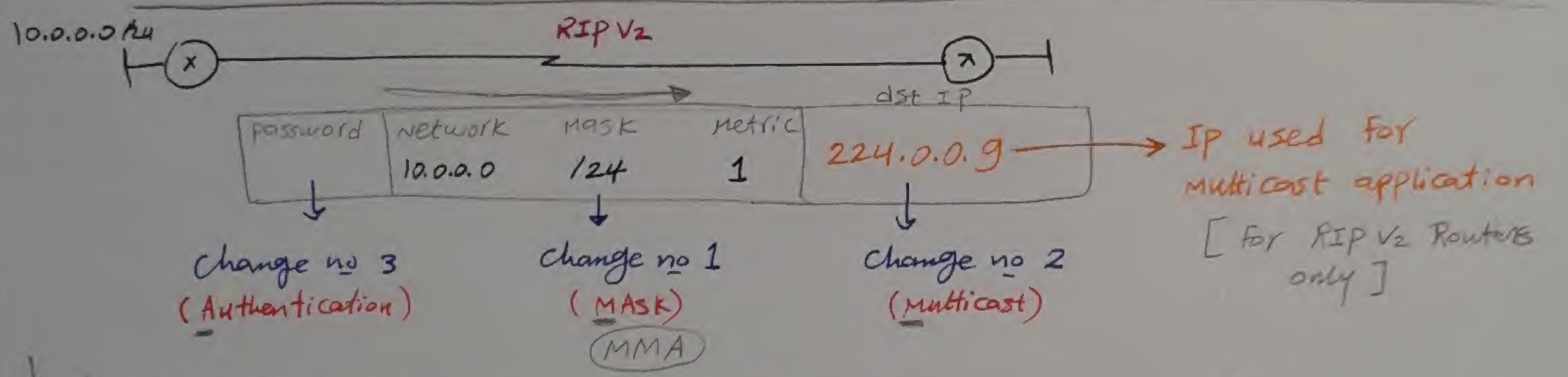
① RIP v2 = RIP v1 + 3 updates change



المشاكل

1. في RIP V1 كانه الـ Network بيتبعت Classfull يعني (doesn't send Mask in updates)
2. الـ Routers بترسل الـ RTG table updates في الـ packet عن طريق العنوان دة 255.255.255.255 (Broadcast) ← المشكلة هنا انه لما تبعت حاجة Broadcast في الـ Network ، انت بتتعب كل الاجهزة في الـ Network انها تعمل process للـ packet دي وبالتالي كل الاجهزة هتشتغل على الفاضي حتى الـ PCs

---



① التغيير الاول / جعل الـ Network من Classfull الى Classless وارسل الـ Mask معاها

② التغيير التاني / حوّل الـ dst ip من Broadcast الى Multicast وبالتالي لما اي Router يبعت update على العنوان دة 224.0.0.9 ← مفيش اي جهاز هيفهم الـ update الا لما يكون العنوان متعرف عنده ما وعشانه اجعل Router يفهم العنوان دة، لازم اسطب له S/W خاص للروتر وامتوله فيه انت شغال RIP V2

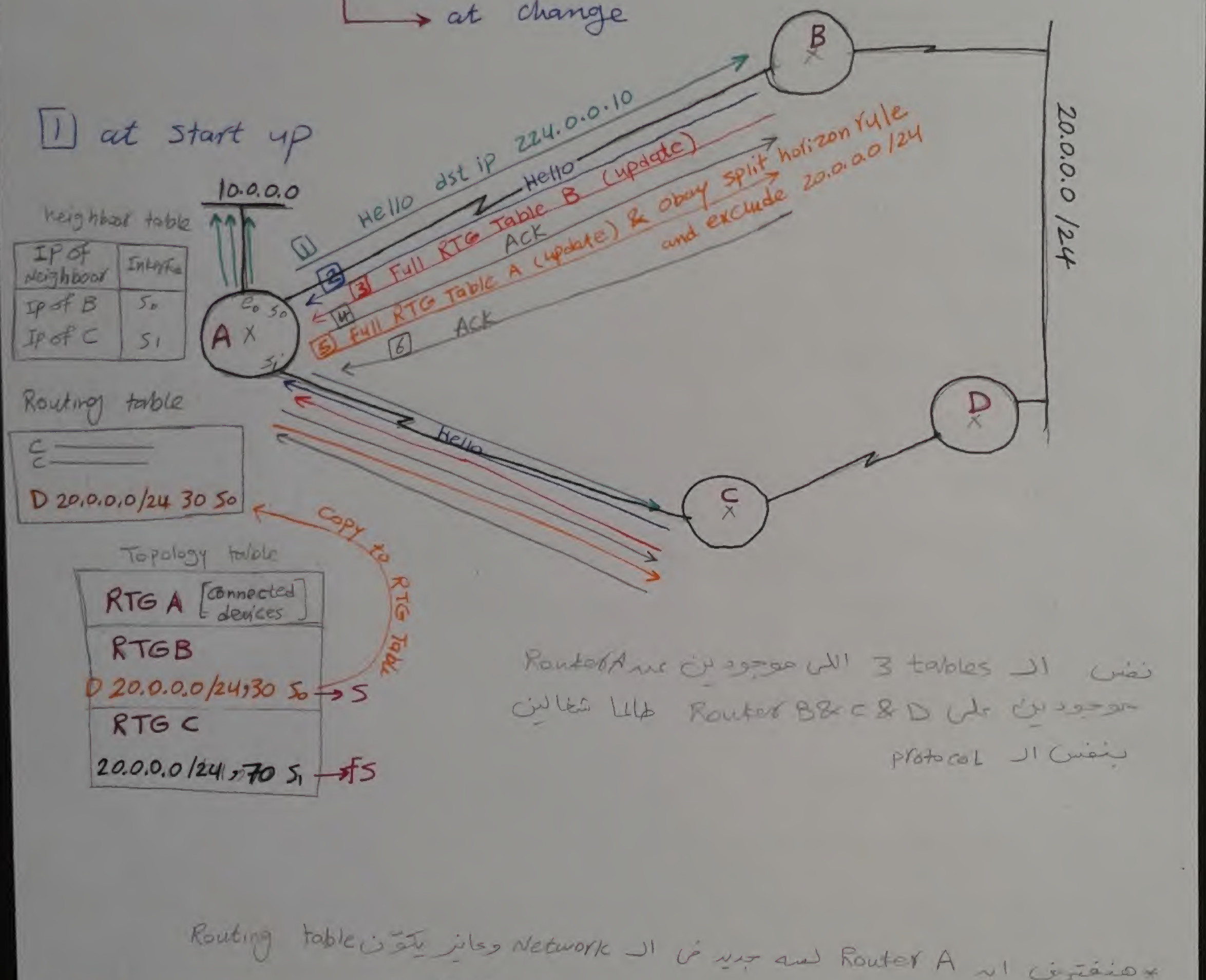
ملحوظة / انا ممكن يكون عندي Routers شغاله RIP V2 و Routers تانية مش شغالة RIP V2 ← ملحوظة/ لو Router شغال RIP V2 وجاله update على عنوان تاني ما هش هيفهمه وهيرميه

③ التغيير التالت / Athentication password وده بحط في كل الـ Routers نفس الـ password وبالتالي لو Router غريب دخل الشبكه وعمل updates وعمية لبقيه الروترات بتاعتي ← الروترات هتعمل check للـ Autho. password ومش هتعمل الـ update

2 EIGRP [Enhanced IGRP]

* EIGRP is type of Advanced D.V
* Its operation → at start up
  → at convergence
  → at change

1 at start up



نفس الـ 3 tables الى موجودين عند RouterA موجودين على RouterB & C & D طالما شغالين بنفس الـ protocol

* متفترض انه RouterA لسه جديد فى الـ Network وعايز يكوّن Routing table
← اول خطوة هيعملها RouterA انه هيبعت Hello msg على dst ip 224.0.0.10
ملحوظة ان الـ Ip دة نوعه Class D يعنى Multicast Ip وبالتالى مش هيفهم الـ Ip دة الا الروترات اللى شغاله EIGRP بس
* ميزة الـ Hello msg ان اللى هيرد على RouterA بـ Hello هيرسله RouterA و هيرسل له update واللى مش هيرد RouterA مش هيرسل اليه الـ update الـ update وبالتالى هيربّح الروترات اللى مش شغاله EIGRP والـ PCs من انها تستقبل الـ upade وترميها [يعنى مش هيخليها تستقبل الـ upade]

* الموضوع ده عملية ارسال Hello Msg عشان ال RouterA يعرف ال Neighbor بتوعه واللي هما ↓

Direct connected ← اللي Routers ال ← ليه Neighbor

understand same protocol

* ال Direct connected Routers اللي حوالينا هما Router B & C

* وطبعاً هيقوم

وده جدول للروتر اللي ردت عليه ↓ Neighbor table بتاع ال Router A

IP of neighbor	interface
IP of B	S0
IP of C	S1

[Exchange of Hello] Hello ↓

Static ← RouterA اللي عملتله 10.0.0.0/24 Network /عرفته

الخطوة التالية / بعد ما ال Router B&C يبعتوا ال Routing Tables بتاعتهم

ل Router A ، Router A تاخد ال Router tables بتاع C & B

وتضيفهم في جدول جوه اسمه Topology table

- ال Topology Table دي بقى عبارة عن Table في ال Routing tables بتاع Router A & Router B & Router C ، وداخل ال Topology Table Router A

DUAL [Diffusion update Algorithm] (اسمها) صيغة عملية حسابية

العملية الحسابية دي بيتم تنفيذها في الحالة الاتية / لو في Network زي 20.0.0.0/24 ، Router B & Router C جوا عنها لـ Router A بس ← Metric مختلف

Metric = 30	20.0.0.0/24 , 30 S0
Metric = 70	20.0.0.0/24 , 70 S1

في المثال بتاعنا RTG B كاتب السطر ده ~ ~ ~ RTG B و

صابق ال DUAL هتشتغل وهتحسب Back up Path & The best path

The best path ← [Successor] وهتحطيه الرمز ده S

الطريق التابع

The Back up path ← [Feasible Successor] FS ~ ~ ~

منه أبوك

* مبسوطش ان الحاجه دى بتتم فى الـ Topology Table
وعشان بقى الـ Topology table هيا خد The Topology table
(successor) Best path بس Copy
وحطيتها فى الـ Routing table. A

الخطوه التاليه / Router A هيرسل Full RTG update لـ Neighbor اللى حواليه
ولكنه فى شرط مهم انه بيشغل خاصيه Split Horizon Rule بمعنى [Router A
هيرسل لـ Router B كل الـ RTG Table بتاعه ماعدا الحاجات اللى اتعلموها من
Router B عنده]

Start up الحمد لله خلصنا

ملحوظه / الـ Backup path موجود فى الـ Topology table فقط
لكنه الـ successor موجود فى الـ Topology table والـ RTG table

---

(2) at convergence

* there is no periodic update as D.V protocols [RIP V1 / IGRP]
* but there is periodic Hello to be sure that all Networks are keep alives [with dead time = 3 * Hello]

→ there are two types of interfaces Fast & slow interface (وده بيتحدد على الـ Technology)

* Fast interface when speed > 1.54 Mbps
* slow ~ ~ ~ ≤ 1.54 Mbps

periodic Hello

every 5 sec for Fast Interface

∴ Dead time = 3 * 5 = 15 sec

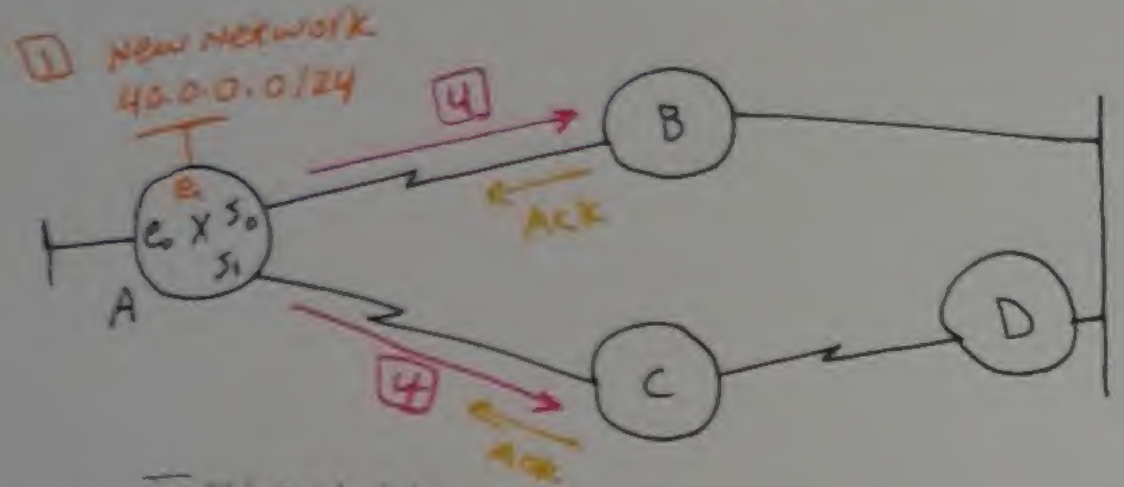
يعنى بعد الوقت ده هيعتبر ان الشبكه وقعت وهيحذفها من الـ RTG Table

every 60 sec for slow interface

Dead time = 3 * 60 = 180 sec

[3] at change

[1] If new network appears :-



Topology table

[2] C 40.0.0.0/24 10 e1 → S (successor)

[3] copy in RTG table

RTG table

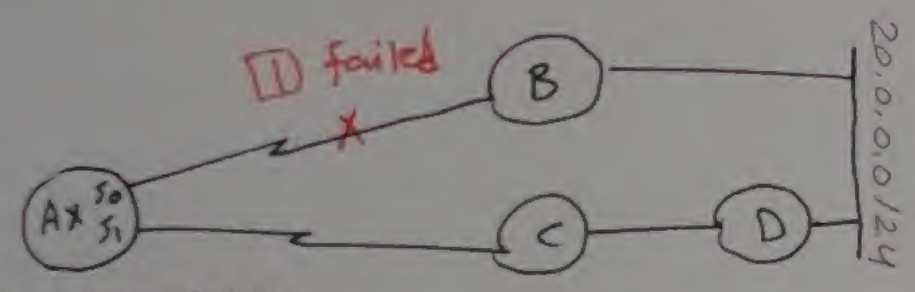
C 40.0.0.0/24 10 e1

[4] send partial triggered update to neighbor
يعني انك عتبعت التعديل الي حصل (الشبكة الجديدة)
[Router B&C] neighbor لـ لحظيا

[5] ⟶ Ack

---

[2] If route fails & there is Back up [FS]



Topology table

[2] ~~20.0.0.0/24 30 S0~~ → S
20.0.0.0/24 70 S1 → FS

[3] copy to RTG Table

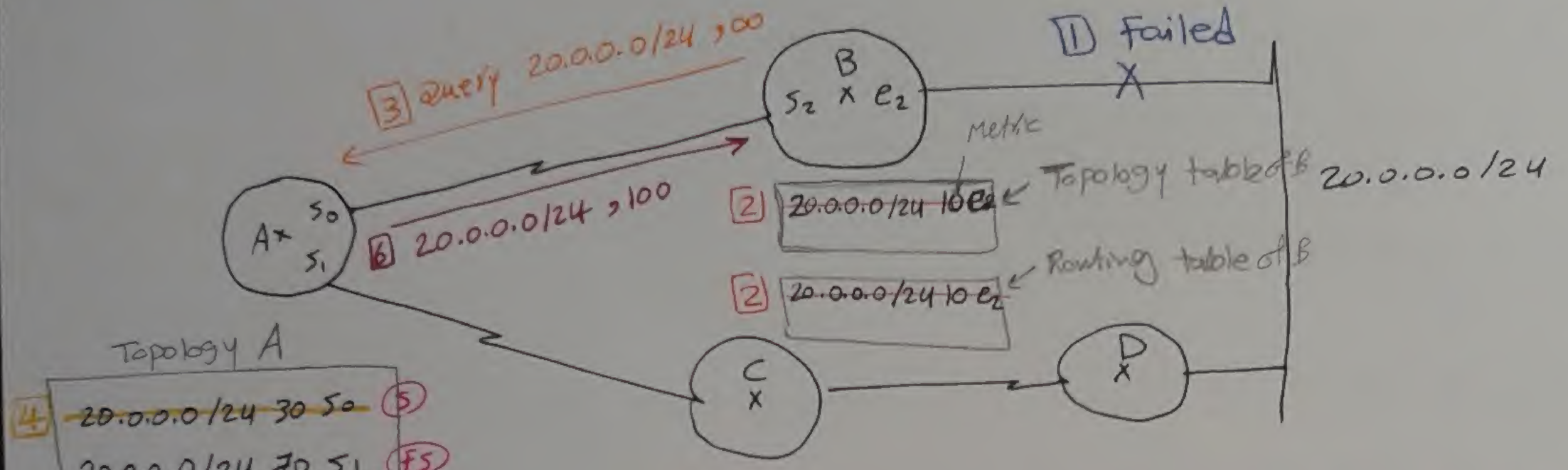
RTG table

[2] ~~20.0.0.0/24 30 S0~~
20.0.0.0/24 70 S1

[4] send partial triggered update to neighbor

Connection failed (1)
(2) حذف من 20.0.0.0/24 30 الـ RTG Table & Topology table
من نفس الوقت
(3) حاخد copy من الـ pack up path في الـ Topology table و سأرسله الى RTG Table
(4) سوف ارسل partial triggered لـ neighbors
بكده بما انى مشغل خاصية الـ split horizon
حتى هينفع | اعلم لـ Router C السطر 20.0.0.0/24 70 S1
عشان انا اصلا واخدها منه

3 If route fails & there is no FS



Connection Failed ①

② الـ RTG table & Topology table بتاع B
جيلو فى الـ Network 20.0.0.0/24 جيلو
pack'up path عندهوش Router B لقيا ←
فى الـ Topology table

③ Router B هيبعت لـ Router A سؤال
بيقوله فيه اله ∞ و 20.0.0.0/24 [يعنى 32bit
اله الـ Network دى وقعت عندى ومابقدرش
اى طريقه تانى ليها] محطوط ∞ عباره عن
32 bit كلهم واحد [1111 - 1111]

④ Router A هيحذف 20.0.0.0/24 30 S0 من
RTG Table و Topology table عنده فى الـ

⑤ ويعمل COPY لـ 20.0.0.0/24 70 S1 (Backup path)
من Topology table الى RTG table

⑦ هيرسل partial trigger replay
to neighboor

وكالعاده مش هيبعتش تحت عشان خاصيه الـ split horizon وهيعرف عند Router B

⑥ Router A هيحسب الـ Metric الجديد بتاع 20.0.0.0/24 70 S1 وهيرسله
لـ Router B [20.0.0.0/24 100 S2]

ملحوظه / الـ Query بيذهب الى اقرب Router خلال 0.1 sec سريع جدا من RIPv1

هو المفروض يبعت الـ Query لكل الـ Neighbors اللى متوصلين بيه

الخطوتين 6 & 7 بيتموا مع بعض

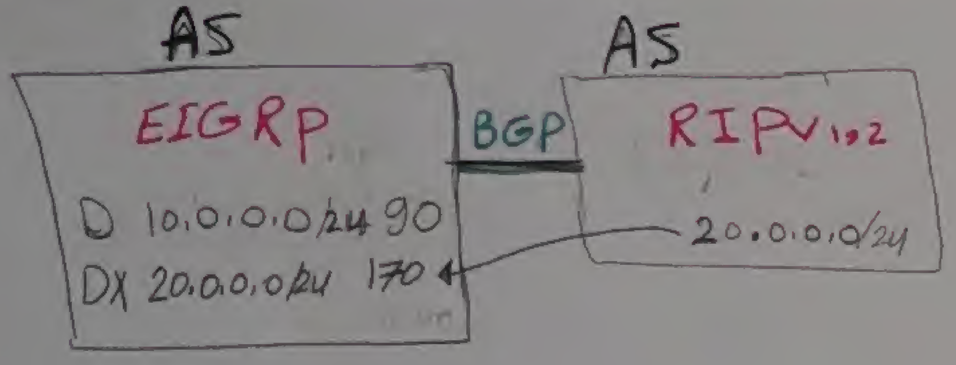
* EIGRP C|C's

[1] it is advanced D.V Cisco protocol
- MASK [classless protocol]
- Multicast [use 224.0.0.10]
- Authentication password [optional]

[2] at start up: send full Routing table once
at convergence: only send 3 periodic Hello
at change: send partial triggeA update → If S fails, use FS
→ If S fails, no FS → send Query

[3] symbol in Table "D"

[4] admin distance = 90 & 170

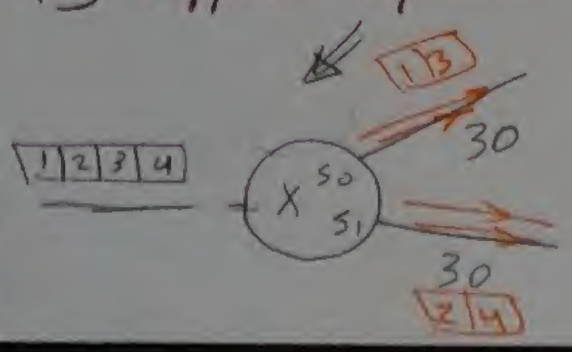


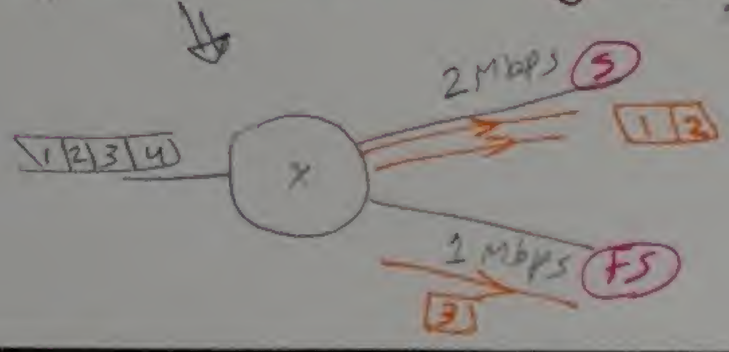
لو 20.0.0.0/24 عايزة تكلم 10.0.0.0/24
اولاً BGP هيحولها من (BGP ← RIP)
ثانياً BGP ~ ~ (EIGRP ← BGP)
وهياخدها EIGRP ، ويعطيها Metric = 170

[5] EIGRP Metric (32 bit) = 256 * IGRP Metric (24 bit)
[BW, delay, load, Reliability, MTU]
default

max no of hops = 224

[6] use DUAL to calculat best path & back up bath
[7] support many routed protocols [IPV4, IPV6, IPX, Apple talk]
[8] support equal & no equal loadsharing [4 paths by default
• mac [16 or more]]





لاحظ انه بقدر يبعت عن طريق الطريقتين مع بعض

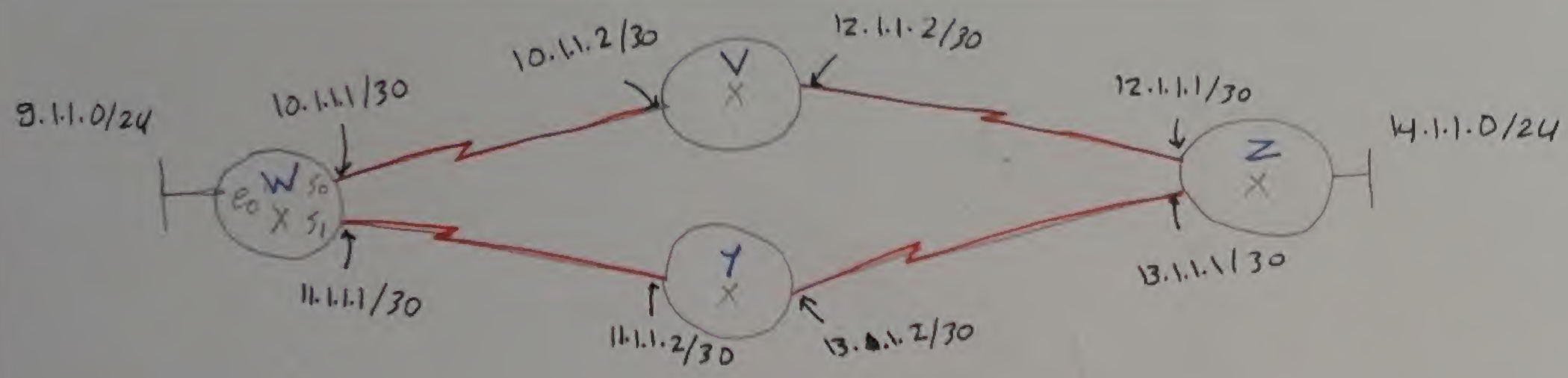
link state

ex : OSPF (open shortest path First)

ISIS

Hybrid [1] D.V [2] link state [3] advanced D.V

∞ EIGRP is Hypred of RIPv1 & link state



[1] at start up (we assume that Explanation about Router W

(config if) # router ospf

(config Router) # network —

[A] neighbor discovery (exchange of Hello)

→ to produce neighbor table

↳ Hello is sent broadcast

Ip of neighbor	Interface
Ip of V	S_0
Ip of Y	S_1

[B] Route discovery (exchange of updates) ⟶ is sent multicast

⟶ LSAs

Each router will form a packet discribing itself called LSA " link state advertisment] and send its LSA to all neighbors

Network / mask	Metric	
9.1.1.0/24	10	Router ID
10.1.1.1/30	10	W
11.1.1.1/30	10	

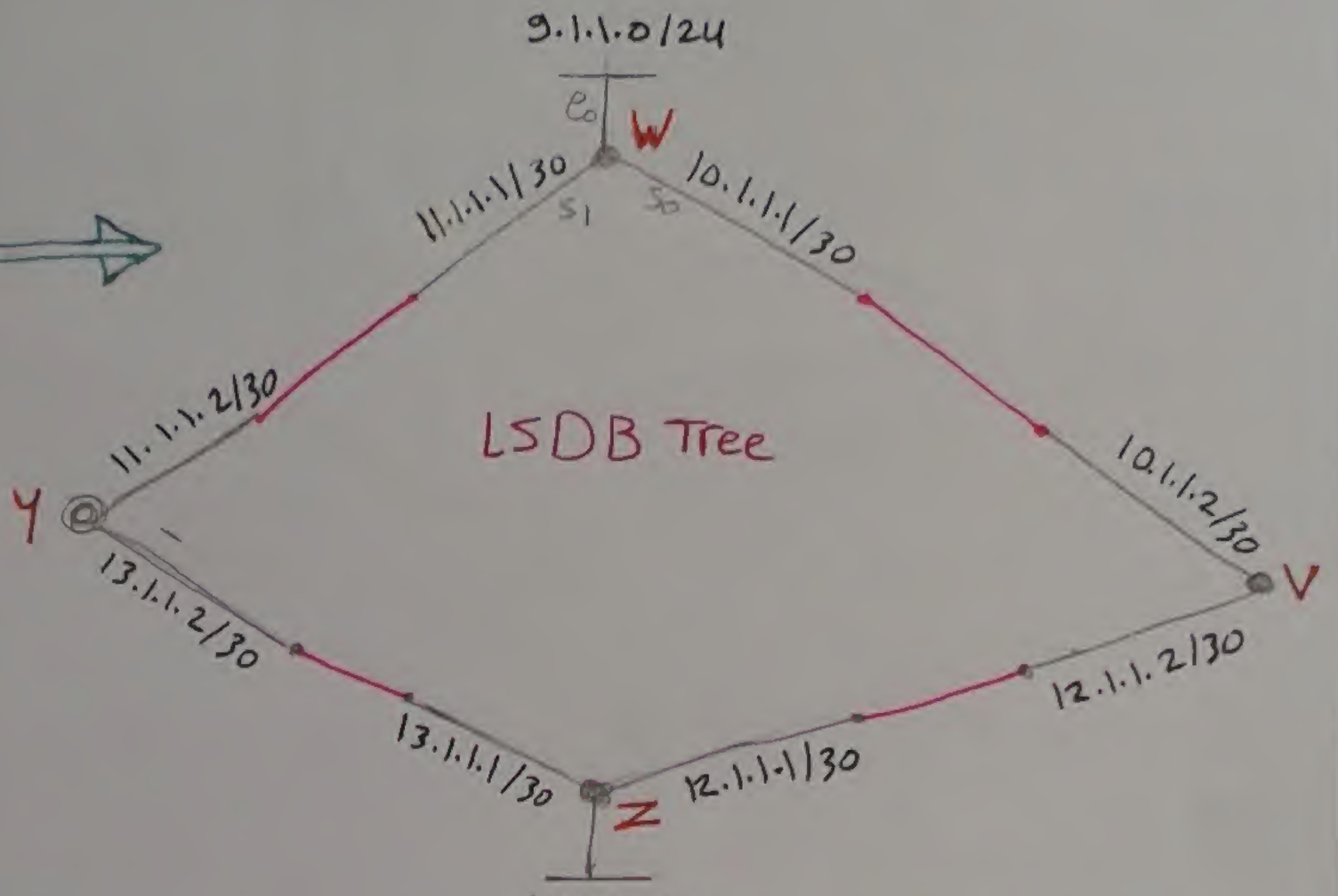
⟹ LSA of W

[C] Each Router that receives LSA will talk a copy of it in its LSDA " link state Data base " and send another copy of LSA as it is to all other neighbors

LSDB (a group of LSAs)

	network/mask	metric
W	9.1.1.0/24	10
	10.1.1.1/30	10
	11.1.1.1/30	10
V	10.1.1.2/30	10
	12.1.1.2/30	10
Y	11.1.1.2/30	10
	13.1.1.2/30	10
Z	12.1.1.1/30	10
	13.1.1.1/30	10
	14.1.1.0/24	10

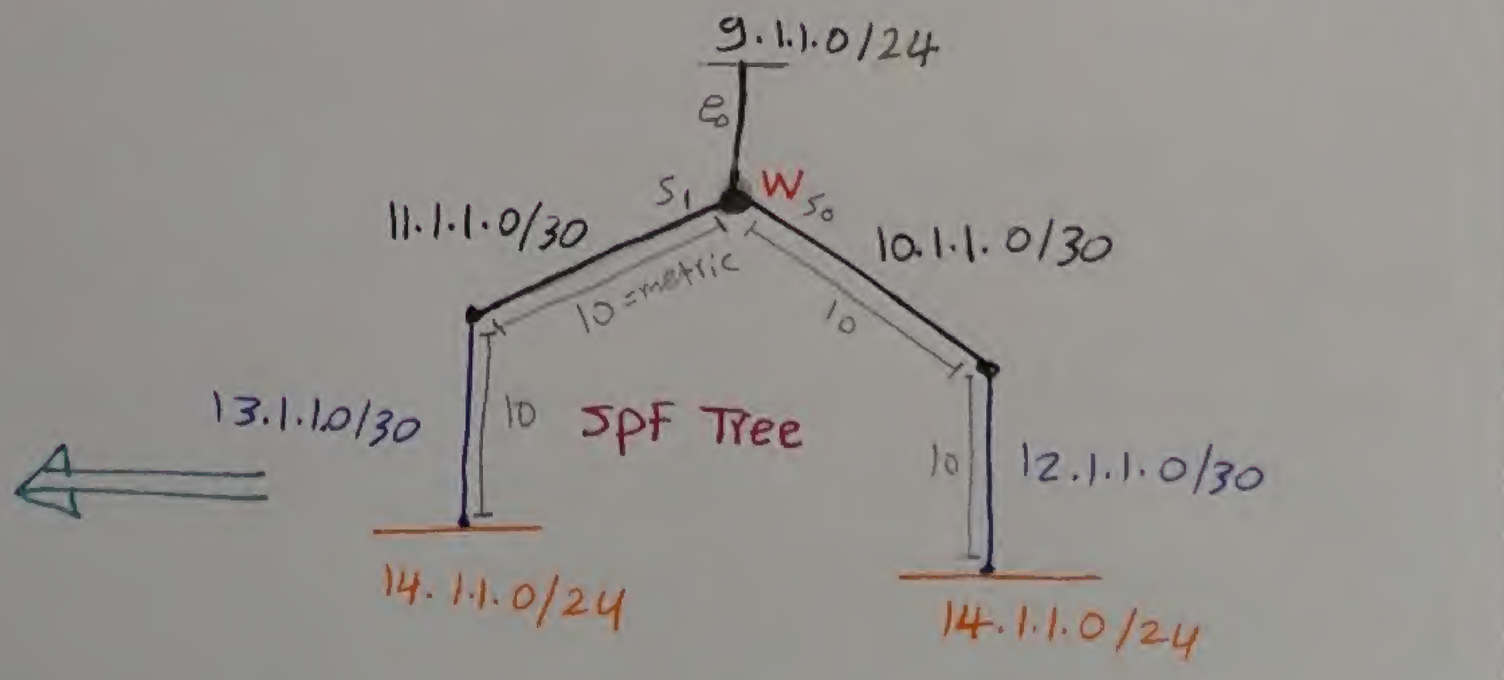
Note/ I take in consideration split horizon



Dijkstra algorithm
SPF [Shortest path First] algorithm

RTG table of W

9.1.1.0/24	e_0	0
10.1.1.0/30	s_0	0
11.1.1.0/30	s_1	0
12.1.1.0/30	s_0	10
13.1.1.0/30	s_1	10
14.1.1.0/24	s_0	20
	s_1	20



LSDB Tree مع SPF Tree الجدول نفسه *
Run 6 process times ناتج

network ل load sharing الجدول يعكس *
مع الرسم 14.1.10/24 (تم)

[2] at change

Router that Feels change will send New LSA discribing its current State triggered to all neighbors

LSA

10.1.1.1/30	10	Router ID
11.1.1.1/30	10	W

← وقتي ① لو 9.1.1.0

② كل Router هيشيل LSA القديمه ويضع الجديدة

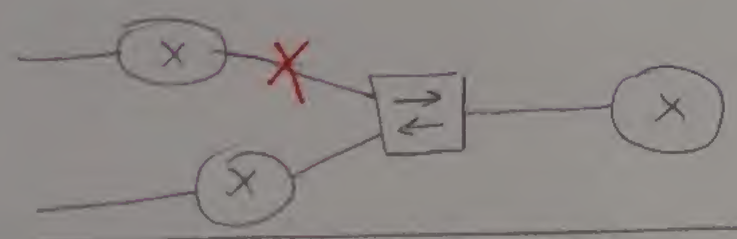
③ كل Router هيعمل Process لـ 5 secs بيبعت فيها لـ 20 Router متجاورين 5 sec بس عشان يرجع الـ Convergence تاني

[3] at Convergence

[A] Send periodic Hello every 10 sec [Hello for 4 times]

[B] Send periodic LSA every 30 minute
it is sent as' LSDB refreshment

يعني لو روترين متوصلين ببعض point to point ، لو واحد وقع التاني هيحس بيه في نفس الوقت . لكن المشكله لو اكتر من Router متوصلين ببعض point to multipoint لو واحد وقع الباقي مش هيحسوا بيه ، عشان كده انا بستخدم periodic LSA ثابتة كل $\frac{1}{2}$ ساعه



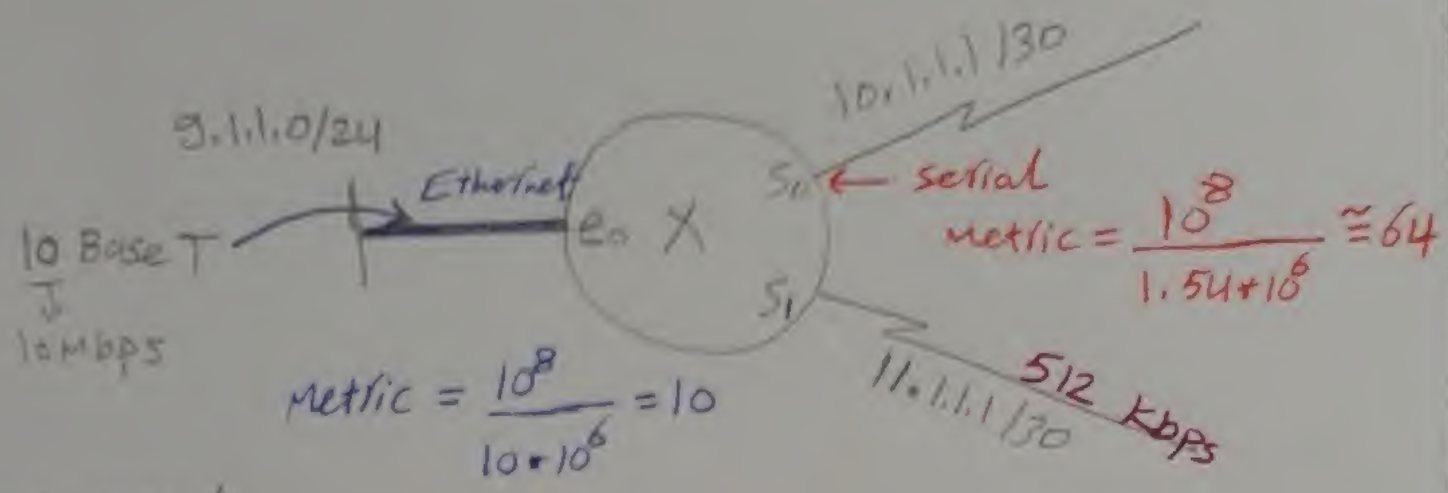
OSPF Ch/C's

1- it is open standard → every one can develop in it
2- Mask [Class less protocol]
3- Multicast [use 224.0.0.5 & 224.0.0.6]
4- Authentication (option)
5- use Dijktra algorithm
6- symbol in Table "O"
8 - admin distance = 110

9- metric ≡ cost = $\frac{10^8}{\text{Bandwidth}}$ [defaut for serial = 1.54 Mbps]

LSA for W

9.1.1.0/24	10	W
10.1.1.1/30	64	
11.1.1.1/30	64	



the defaut / the router set any serial port by metric 64 [defaut], unless you set the speed by yourself with this order (config-If)# bandwidth 512
↓ in units of Kbps

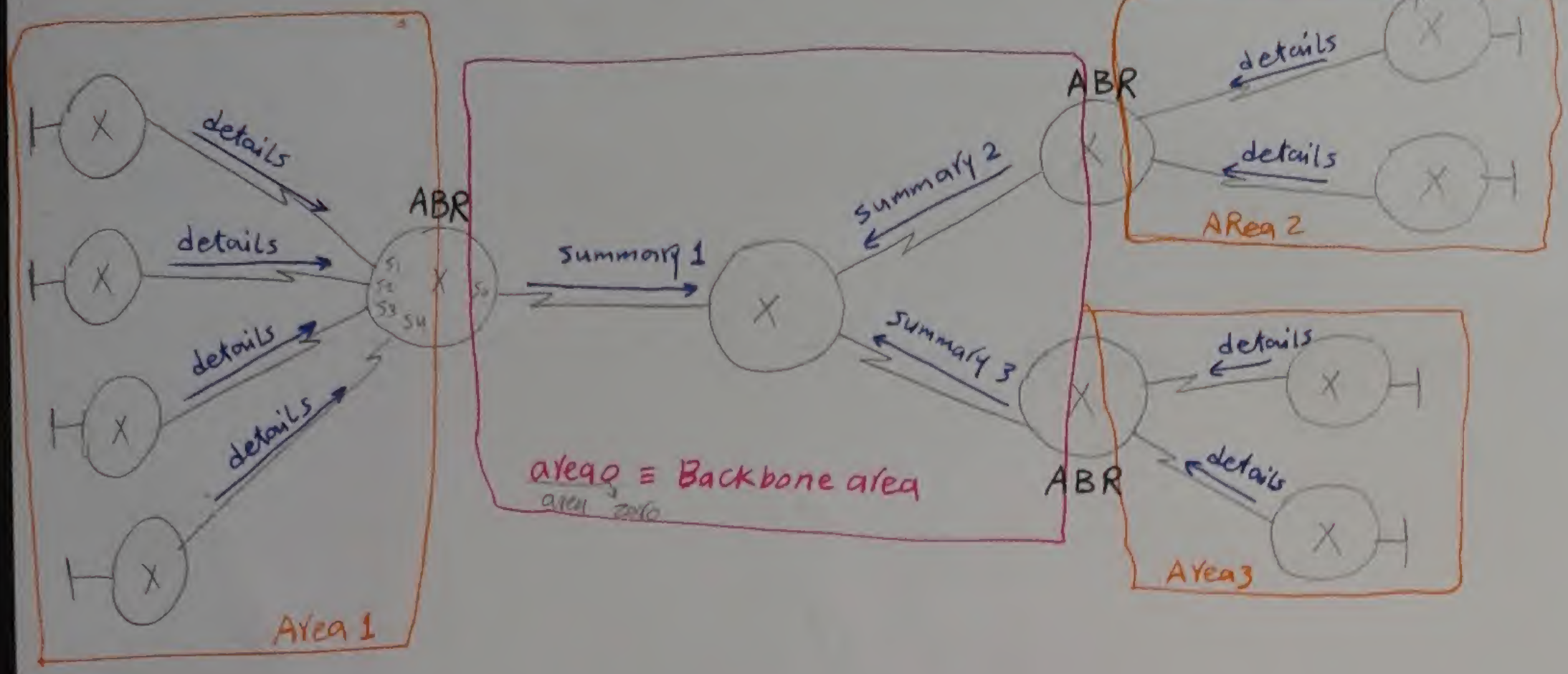
10- Hierarchical design (multiple access ospf)

* before Hierarchical design

1. need high processing
2. need big memory
3. instability affect intire (كل) AS (autonomos sys.) (as Flapping الرفرفه)
4. Complex [design, Implementation, configuration]

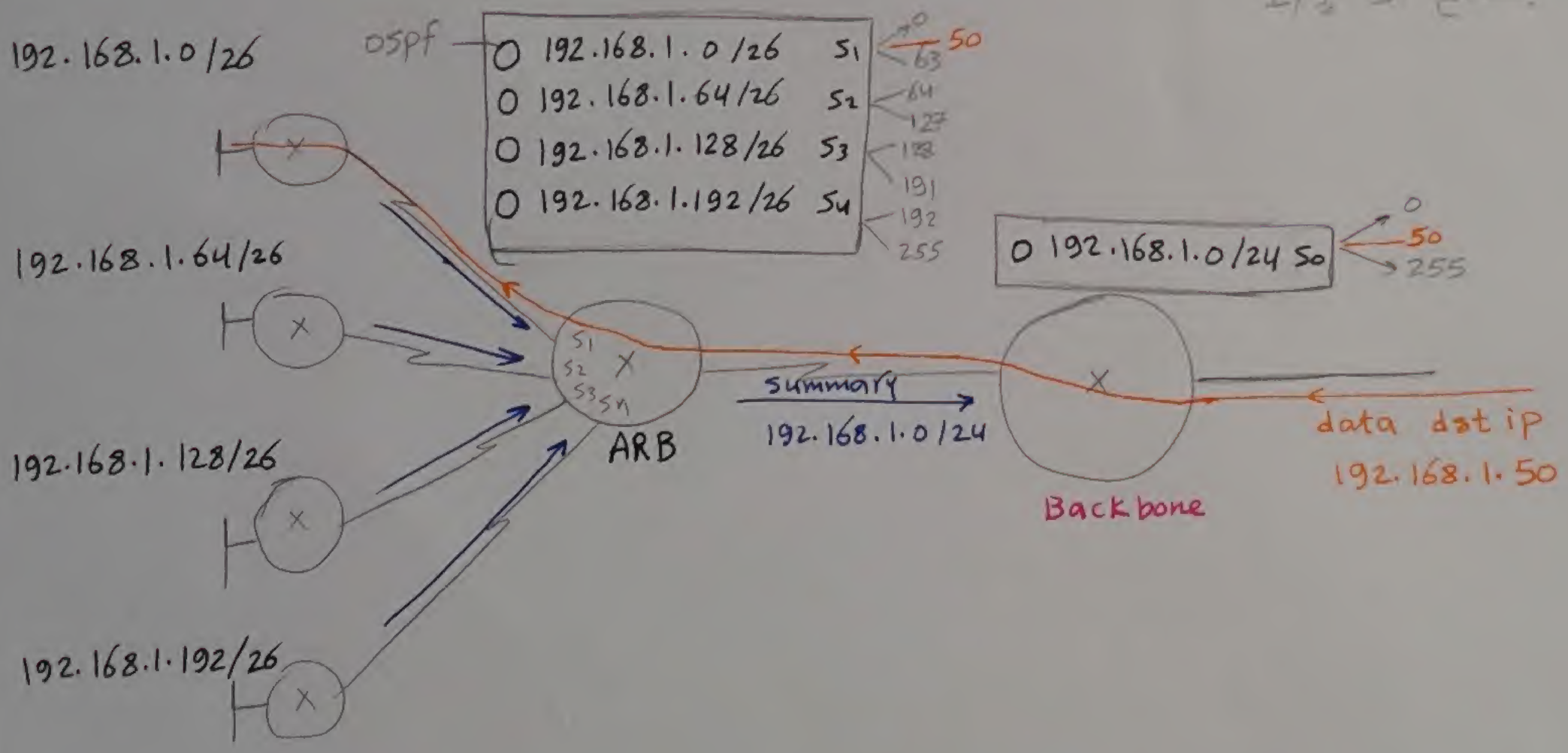
The solution is :- Deviding AS into sub AS's called Areas
(If no of Routers > 50)

Area :- Each area contain and know all details about Routers in that area and summary only about other areas.



ABR : Area Boarder Router / it is responsible for taking details from all interfaces and outcome the summary of one interface

* انت رتبت الروترات اوى بتكبر الـ Design هيكون complex بالنسبالك وانت بتنظم الـ IPs



Note Home Router

0.0.0.0/0 ⟶ H = 32

∴ 2^{32} = all

* Route summarization & CIDR [Classless Interdomain Routing]

* Route summarization / grouping subnets and advertise them as single Major Network
* supernetworking / grouping Major networks and advetrise as supper network (CIDR)

Common → /25

192.168.1.128/26
192.168.1.192/26 ⇒ 192.168.1.1 000 00000 / 192.168.1.1 11 00 00000 → 192.168.1.128/25

* In RIP v2 & EIGRP

⟹ by defaut auto summary in them

[discontiguos network (المشكلة اللي هتحصل هنا اسمها)

* لو الـ Router وجد اكتر من Network بتبدأ بعنوان ثابت ، الـ Router بيبص لأول Octet من العنوان ده و بيحدد ClassA / ClassB / ClassC ، وعلى اساس نوع الـ Class بيقطع الـ Mask ، لكن المشكله زى الرسمه وهما عندهم interfaces على Router A متوجه

ClassA هيعتبر انهم RouterA ⟸ 10.2.2.0/24 & 10.1.1.0/24 ← وبياخد summary

الـ Mask ⟸ 10.0.0.0/8 و Router C نفس الوضع هياخد summary بنفس الـ Mask

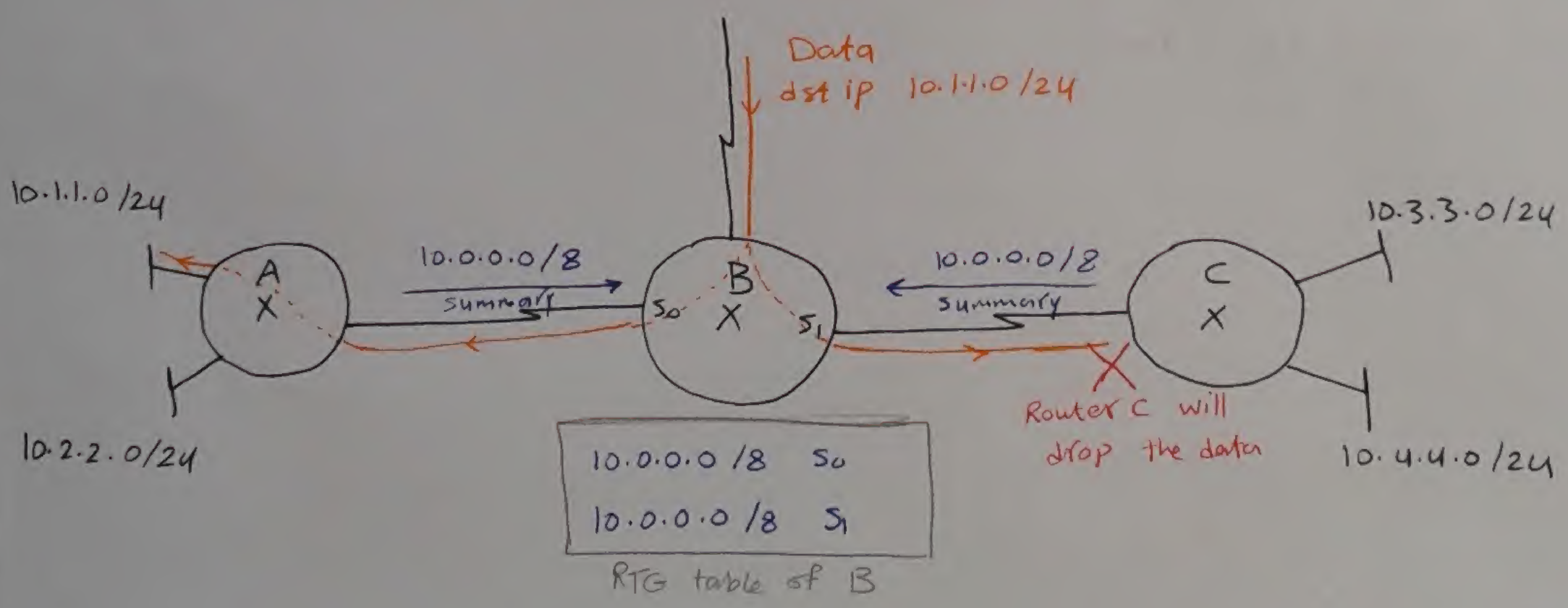
وباسم الـ Network

⟸ هيبعت Router B وهيعرف انه عنده 10.0.0.0/8 متوجه على 2 interfaces (S0, S1)

وبالتالى لو ذهب له dst ip 10.1.1.0/24 هيعتبر انه الـ 2 interfaces بيوصلوا لنفس الـ distination وهيعمل load sharing ويقطع جزء كبير من الـ packets

⟸ حل المشكله دى انك تلغى خاصيه الـ auto-summary بالأمر ده

(config-router)# no auto summary

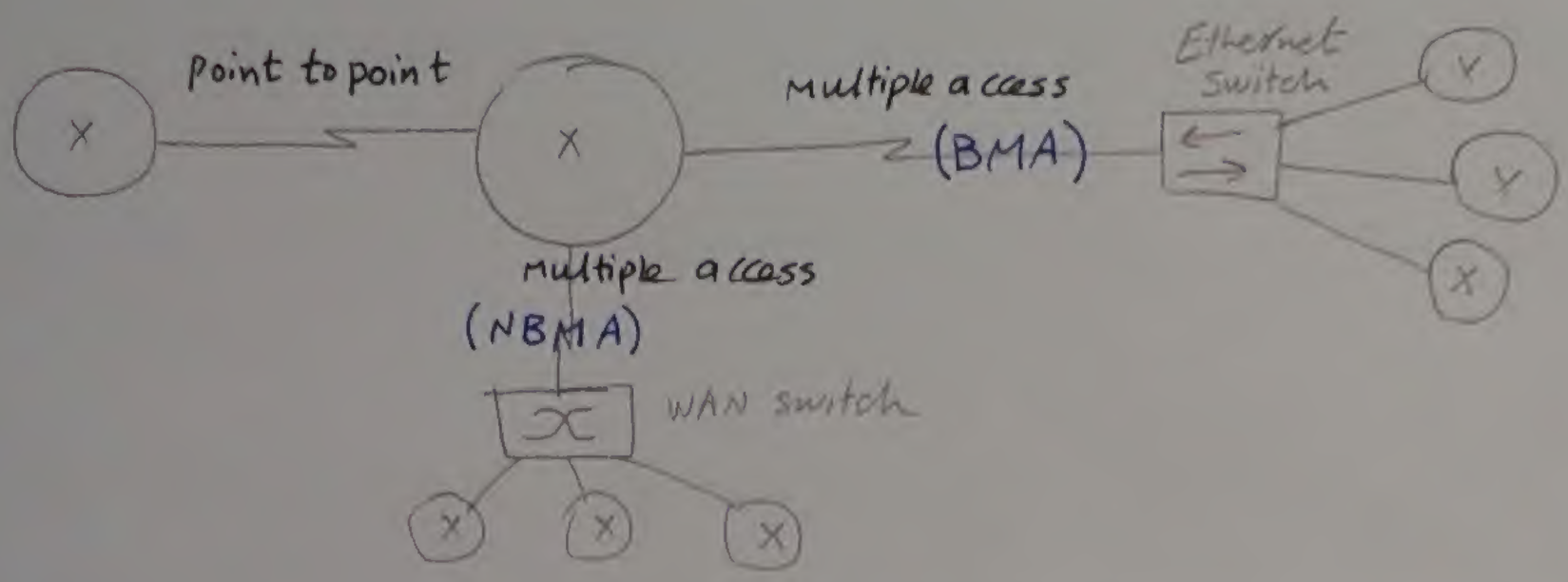


10.0.0.0 /8	S0
10.0.0.0 /8	S1

RTG table of B

* ospf topologies → point to point
→ point to multipoint [Multiple access]

* Multiple access → BMA [Broadcast multiple access] used in LAN
→ NBMA [non Broadcast multiple access] used in WAN
يعني اني مفيش Broadcast في الـ WAN

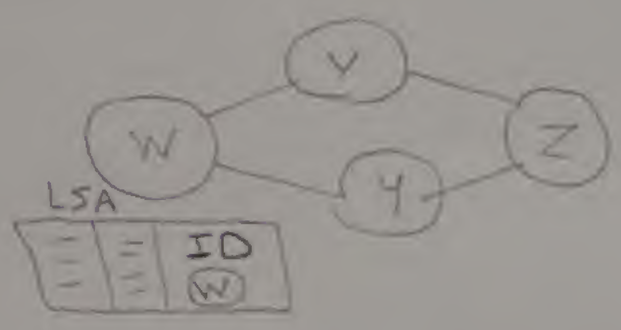


---

* OSPF operation in Multiple access

at start up : (config) # Router ospf #

[1] Router ID [RID] : 32 bit
الافضل انه يكون private



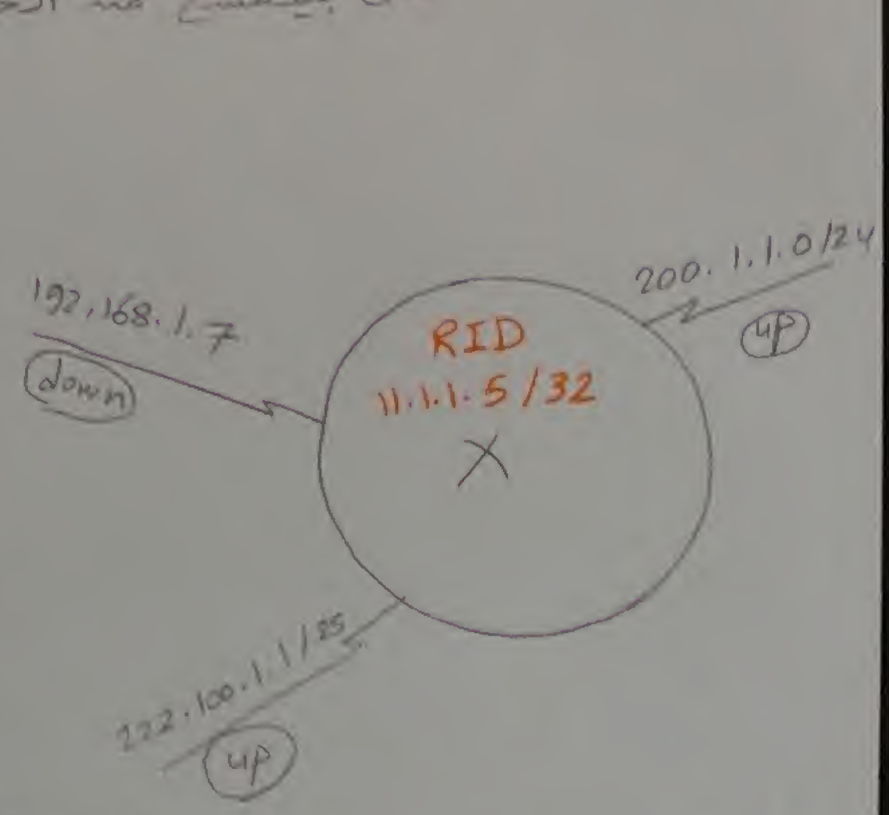
② it is the highest IP address configured on loop back Interface

internal s/w logical vertual always up → means no shutdown
يعني اني لو الجهاز اتطفى و اتفتح تاني
مش بيتمسح من الجهاز

* you introduce ID Manually
* adv. → it is more stable
الارسى

(config) # interface loopback 0
غيره بأي رقم

(config-If) # ip address 11.1.1.5 255.255.255.255
ID Host Mask

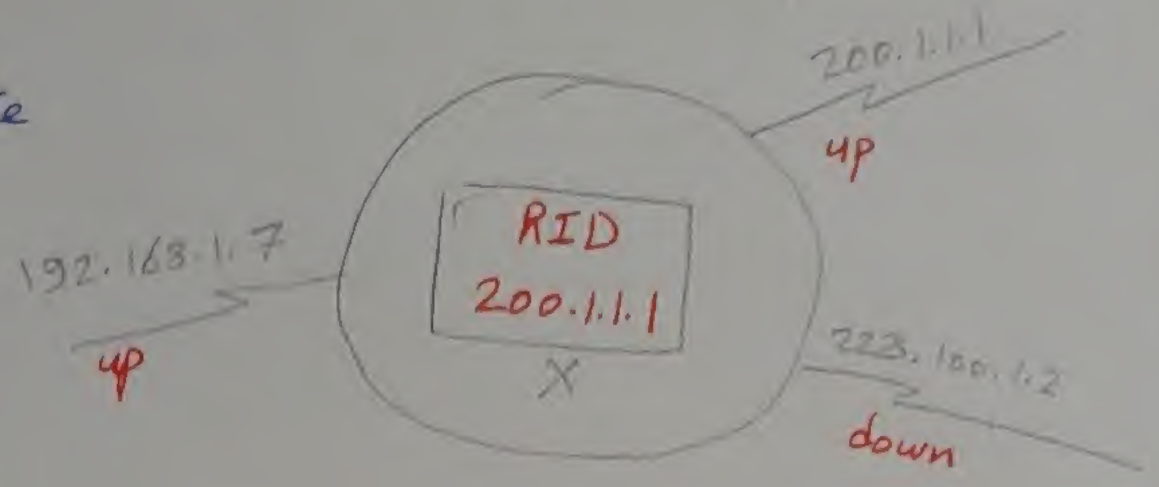


Note/ Mask → /32 ∴ H = 0
∴ no of IPs = $2^0 = 1$
∴ this IP is the only on of his subnetwork → we don't wast IPs

Home Router
لازم اعمل تعريف قبل ما ادخل IP بتاع الـ

(b) it is the heighest Ip address configured on physical active interface

Ethernet serial



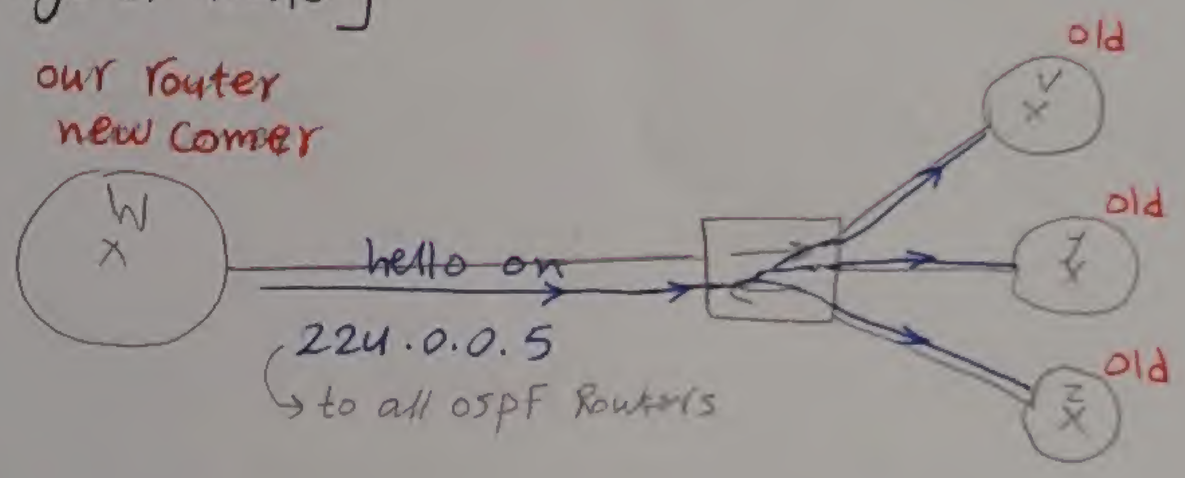
* وهنا اول ما الـ Router بيفتح بينظر ان كل الـ Interfaces اللي عليه [up] وبعدين هيشوف Ethernet ولا serial
اكبر IP عندهم وياخده كـ (ID) لنفسه والـ ID دة بيكون ثابت لـ Router
[حتى لو الـ Interface دي فصلت (Down) طول الوقت (الاغلب حالة) الـ Router كله فضل فاكرها هيبقا هي جديد يدور على اعلى IP [up] وياخده ID جديد لنفسه

ملحوظة/ اول حاجة بيعملوها الـ Router عشان ياخد ID هو انه يدور الاول على loopback interface ولو ملقاش هيدور على اكبر IP serial interface عندة وياخدة ID

[2] Neighbor discovery [Exchange of Hello]

* hello is sent Multicast to all neighbors on this IP [224.0.0.5]

: The routers that configured OSPF protocol can only receive this Multicast IP [224.0.0.5]



The neighbors of new router won't receive the hello msg Except with these conditions :-

① Authentication passord [password]

② Same area to be sure that the new router is our neighbor

③ same hello interval = 10 sec [defaut] but it can be changed by configurat

④ same dead interval = 4 hello = 40 sec

LSA= هيبعتولها Router V,Y,Z و Hello بيبعت Router W لـ اول ما الاتنين دول يكتشف الـ router W بيبقا عندهم 3 LAS= متكررين عشان الاتنين دول هيشتغل على الـ processor بتاعهم وهيعمل الـ memory على الفاضي عشان يبعت تاني الجدول ده DR (الرئيس) و الـ BDR [نائب الرئيس]

[3] Routes Discovery [Exchange of LSAs]

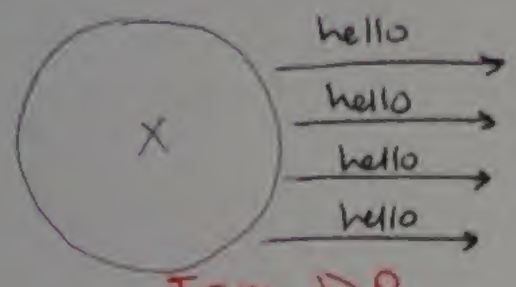
before Routes Discovery there is the electing of DR & BDR

الروتر المسؤول (الرئيس) — نائب الرئيس

[2] Electing Designated Router [DR] & Back up DR [BDR]

DR is

[a] first router to boot ospf with enough time



(40sec) 4 hello لو مفيش حد رد بعد
هيقول انا الرئيس

← لو فى 2 Routers قاموا فى نفس اللحظه هنروح لخطوة [b]

[b] Router having hieghist periority on interface

* periority (0 – 255) the higher the number, the higher the periority
* The periority in all Routers = 1 (by default), you can change the periority by configuration
* periority 0 ⇒ can never be DR or BDR, and it will be [DR other]

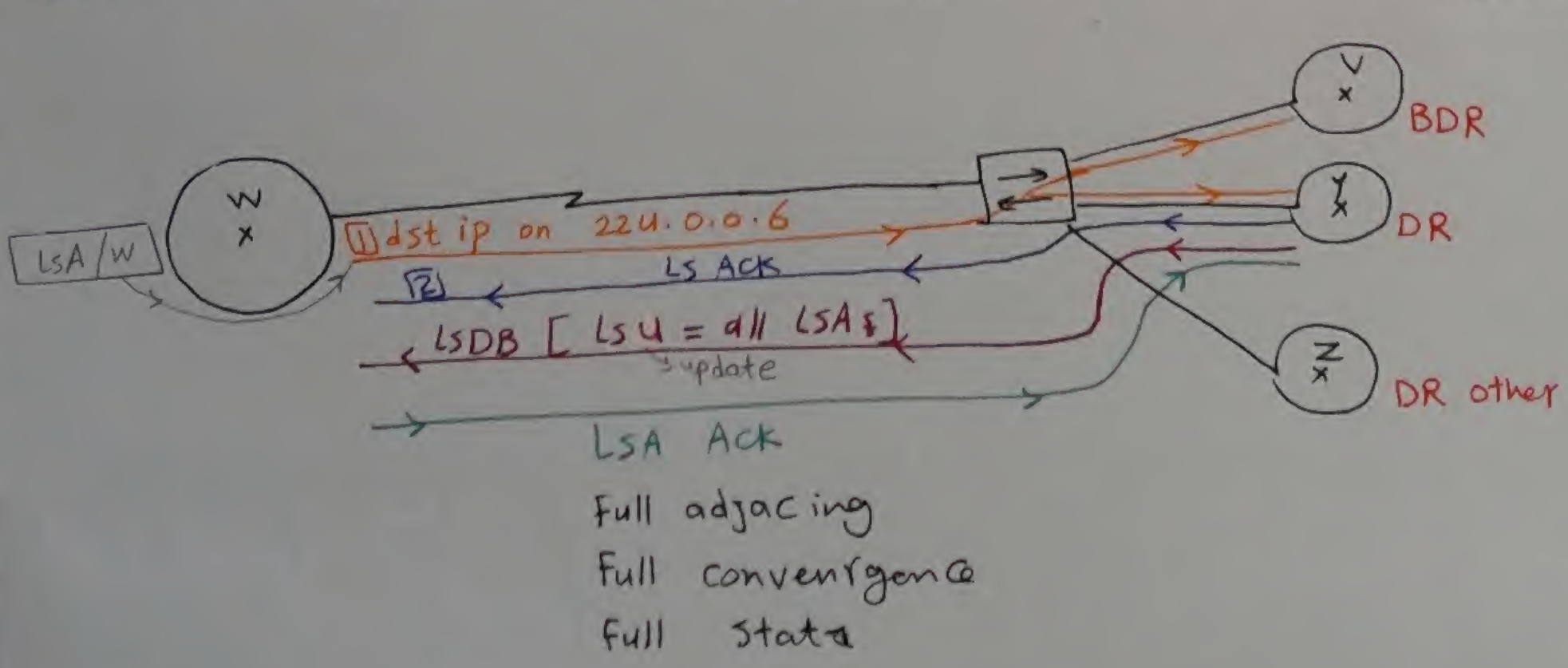
← لو اكتر 2 Routers لهم نفس الـ periority هنروح لخطوة [c]

[c] Router having highest (RID)

* مش معنى ان الـ Router له اعلى RID فانه افضل واحد لكنه لازم يعمل كتة عشان نه نشتغل

224.0.0.5 → to all neighbors to say Iam a live
224.0.0.6 → to DR & BDR only

الاتنين بيبعت Hello عليهم Multi cast ←

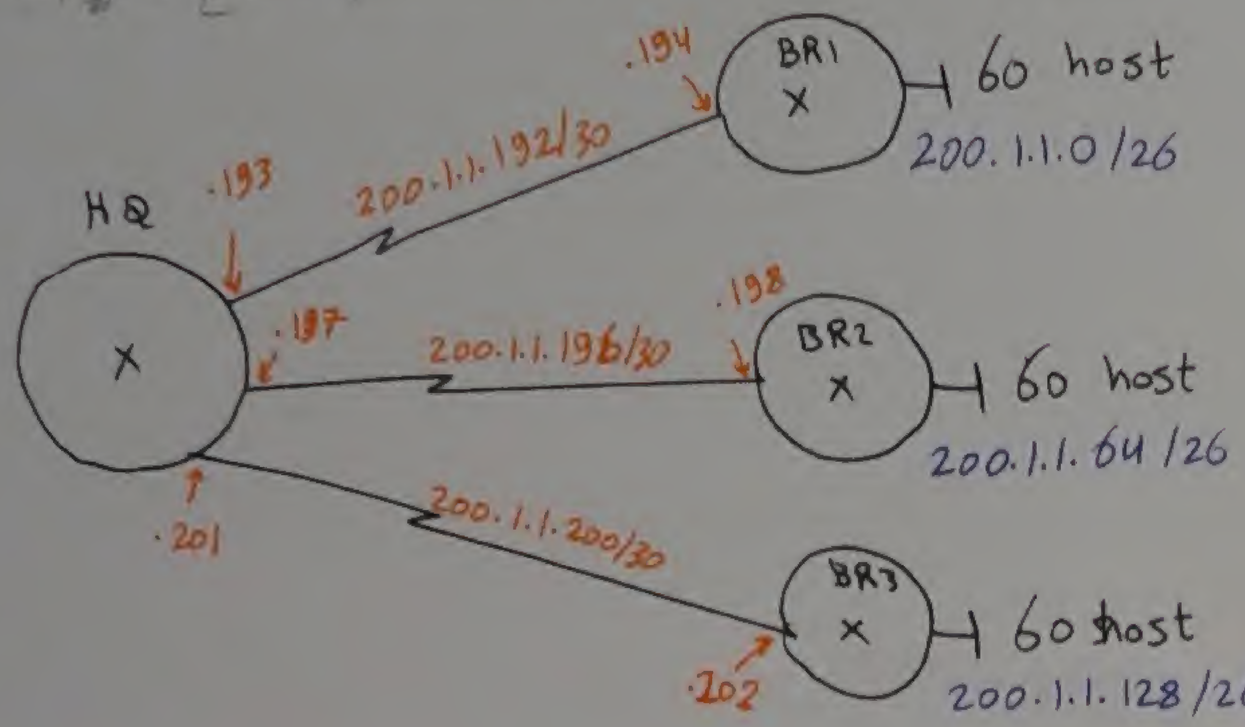


Full adjacing
Full convenrgence
Full State

BR : branch
HQ : head QUARTER

* VLSM [Variable length subnet mask]

انت عندك 200.1.1.0/24 وعايز تقسمه وتوزع الـ IPs



IP محتاج كام ؟

(60+2)
+(60+2)
+(60+2)
+(2+2)
+(2+2)
+(2+2)
→ 198 IP

* انت محتاج 3*62 IP ← هتشوف اقرب Host جتاله بعطيك اقرب رقم من 62IP

مناسب جدا

ob $H = 6 \Longrightarrow$ no of IPs $= 2^H = 2^6 =$ (64 IP) ← hoppa

↳ H=6 ومنه N=26

200.1.1.0/24

200.1.1.0(hoppa)/26 — 200.1.1.0/26

200.1.1.1*(hoppa)/26 — 200.1.1.64/26

200.1.1.2(hoppa)/26 — 200.1.1.128/26

200.1.1.3(hoppa)/26 — 200.1.1.192/26

* you want 3*4 IPs ⟹ (4 IPs) hoppa ⟹ $2^H = 2^2$ ⟹ H=2 ⟹ N=30

200.1.1.(192+0*hoppa)/30 — 200.1.1.192/30

200.1.1.(192+1*hoppa)/30 — 200.1.1.196/30

200.1.1.(192+2*hoppa)/30 — 200.1.1.200/30 ------

Q: which Routing protocols can support VLSM & CIDR ???

Ans :- classless protocols [RIPv2 , EIGRP , OSPF , ISIS , BGP]

حاجه بتقسم Mask يعني بتبعت Mask في الـ update

ماعدا [RIPv1 , IGRP] ← classfull مبيقبلش mask

BGP بين AS مختلفين

EIGRP , OSPF , ISIS في نفس الـ AS

[enable by default] ← (Ip subnet-0) بيقبل فيه الامر ده

(no Ip subnet-0) no بتلغي الامر

* New subnetting standard

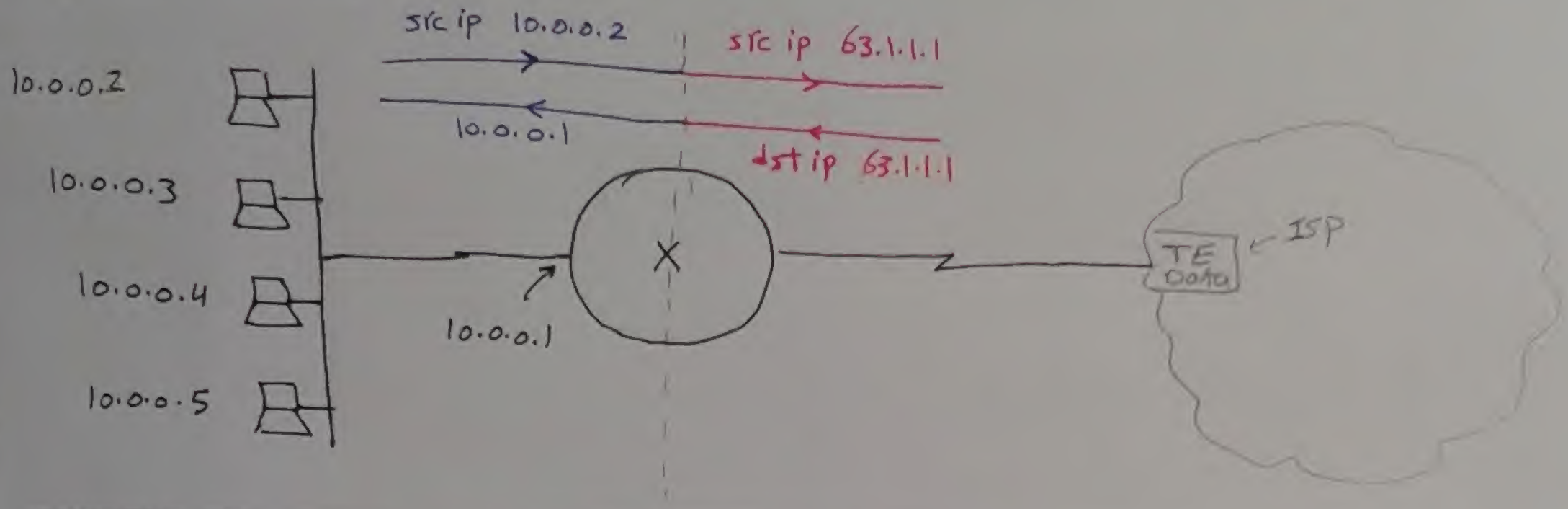
* old subnetting standard

* بتسيب اول واخر subnets لـ Future

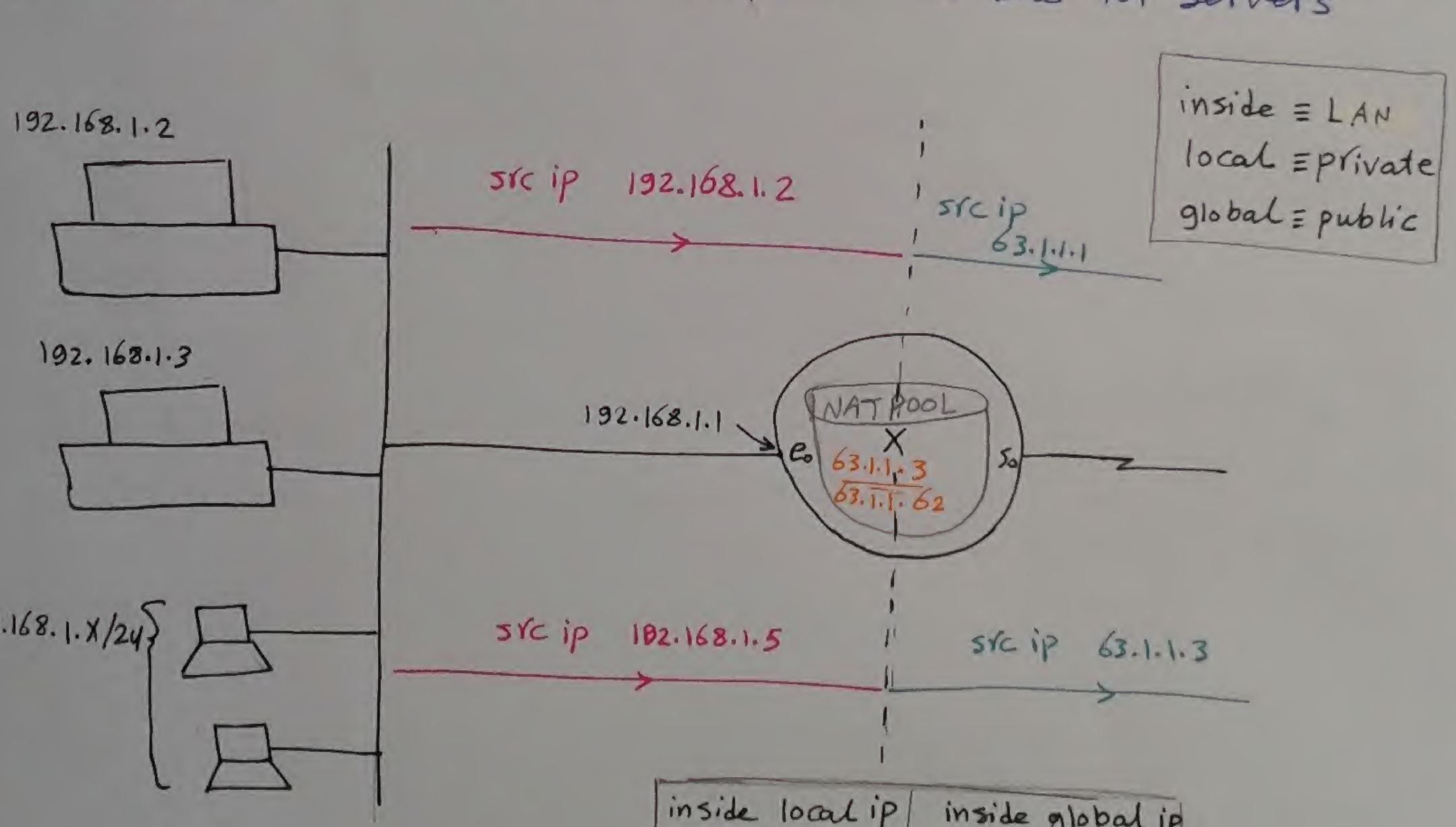
* NAT [Network address Translation] ISP : internet service provider

private IPs :-

10.X.X.X
172.X.X ⟶ 172.31.X.X
192.168.0.X ⟶ 192.168.255.X



[1] Static NAT : 1 private ≡ 1 public ⟶ used for servers



inside local ip	inside global ip
192.168.1.2	63.1.1.1
192.168.1.3	63.1.1.2
192.168.1.5	63.1.1.3

* ملحوظة/ ال servers مفيهاش توفير في IPs لأن ال server لازم يكون له IP ثابت ومعروف ما بالنسبه لو PC عايز يدخل النت بياخد اى IP من ال (NAT pool) ويدخل بيه وانا هنا بفترض انه مش كل ال PCs هتدخل على النت في نفس الوقت

ال PC اللى هيدخل 5 min صغير ما يدخل على حاجه جديده يمكن ياخد منه ال IP بتاعه واحطه في NAT pool

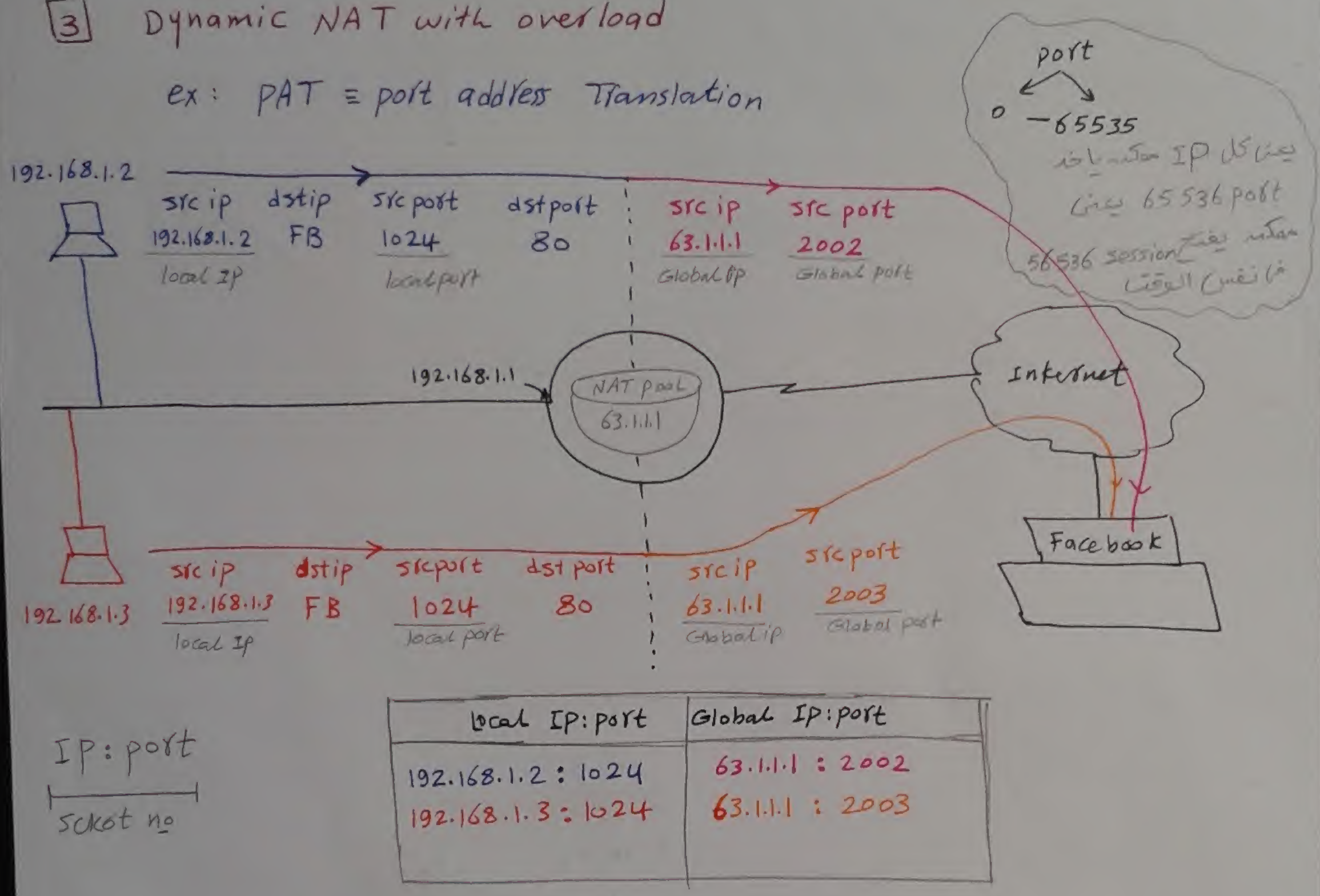
[2] Dynamic NAT

used for users many users ⟶ less public

---

[3] Dynamic NAT with overload

ex: PAT ≡ port address Translation



IP : port
socket no

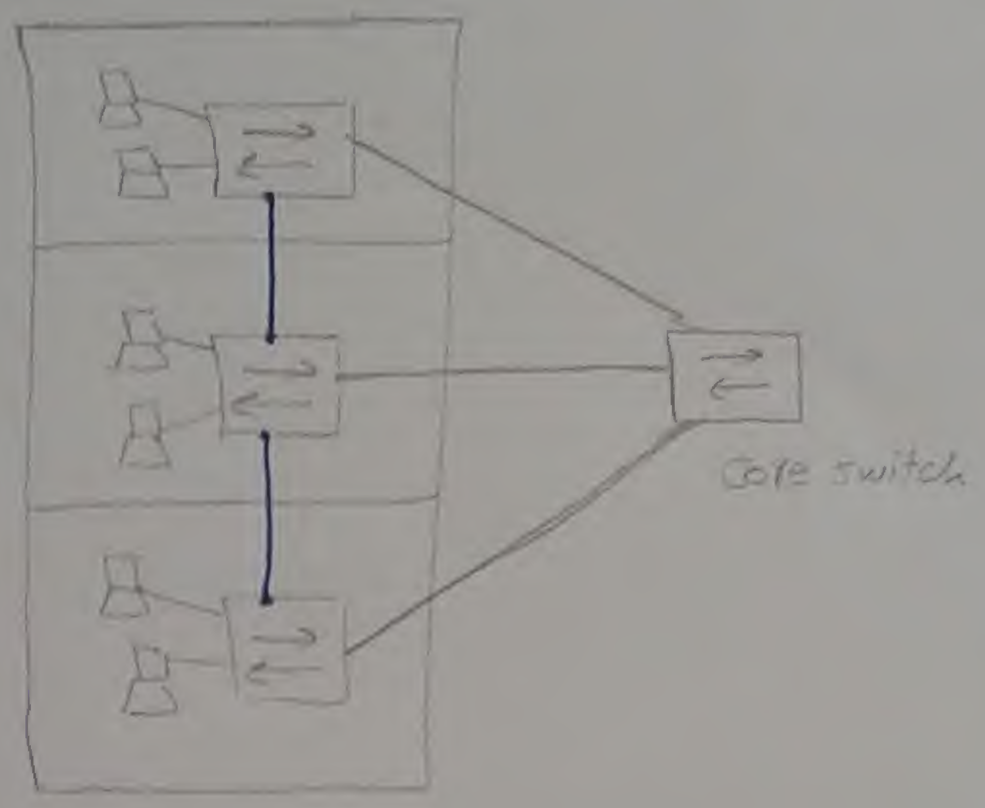
local IP:port	Global IP:port
192.168.1.2 : 1024	63.1.1.1 : 2002
192.168.1.3 : 1024	63.1.1.1 : 2003

one public IP ممكن يستخدمه PC اكتر من التخصيص ، وهنا اكتر من فكرة

Session 16

Switching

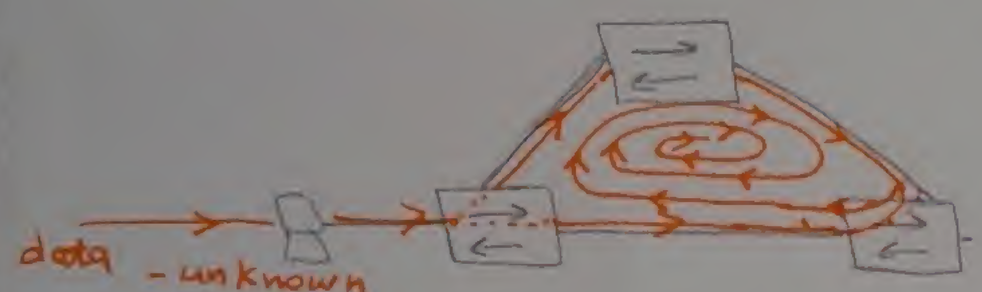
سويتشاً انا مفترض اه كل شغلي LAN



تحليل الشكله

* عشانه ازيد الـ redundancy بتاع الشبكة [لأن لو cable اتقطع هتكونه النتيجة اه كل الاجهزة اللي وراه هتفصل] انا محتاج اضيع Stand by Cables [الوايرز الزيادة]

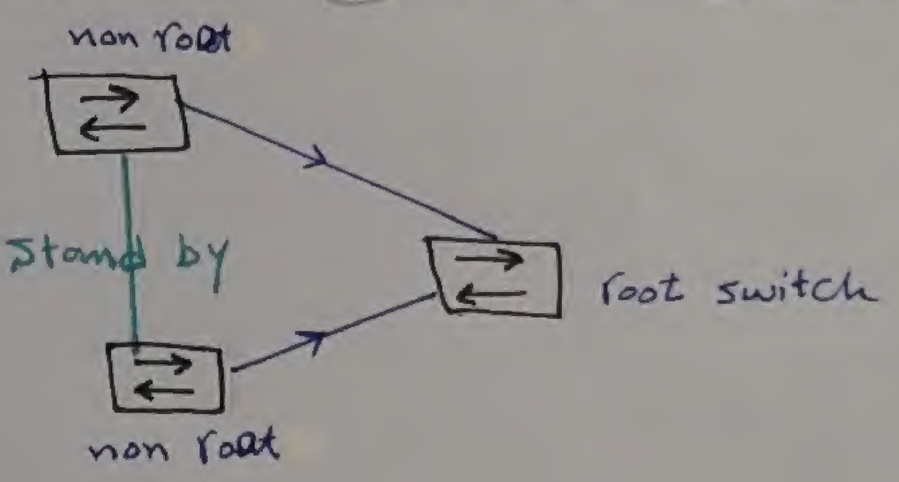
* التبسيط بين ٢ سويتشات فقط



* لو في جهاز بعتين بيرسل Data نوعها unkown / multicast / Broadcast هيحصل loops كتير وهيسبب Broadcast storm

* لو عدد الـ Cables ≥ عدد الـ Switchs ⟸ هيكون loops

عشان كده الحل هيكونه في استخدام [Spanning Tree algorithm] STA



* STP [Spanning Tree protocol] IEEE 802.1 d صنا الـ algorithm دة هيخلي طريقه Backup والتاني pest ولو وقع الـ pest هيتشغل الـ Backup

[I] at start up

① BPDU Flooding :- (Hello Flooding)

* each switch will form a frame describing itself called BPDU [Bridge protocol Data unit] or you can say [Bridge Frame] and send it out out of all interfaces every 2 sec

في الاول كل الـ switchs بتبعت BPDU لحد ما يتتخبوا ريس

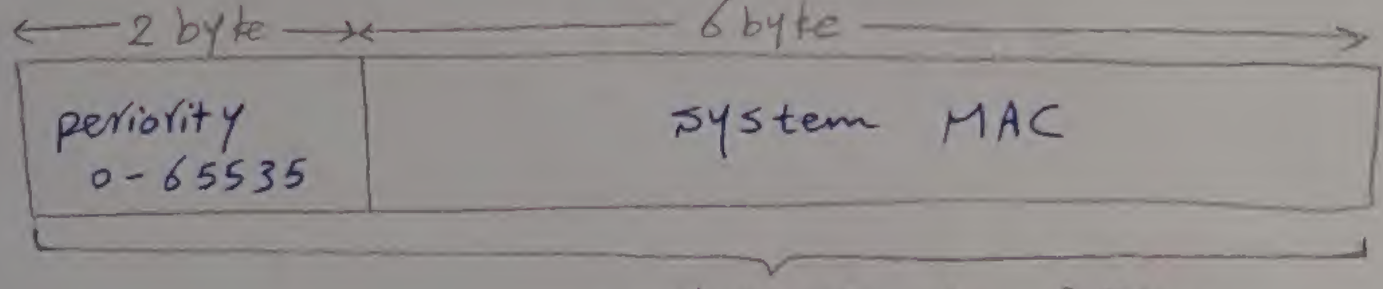
BPDU

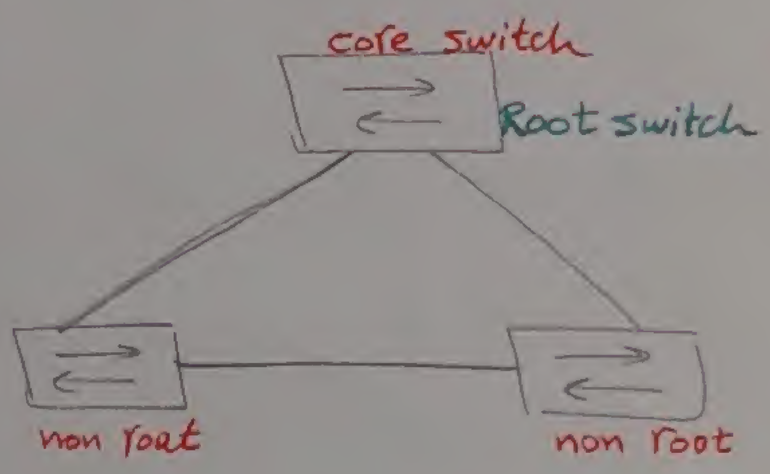
port ID	accumulated path cost	switch ID

(2) Electing root switch انتخاب الرئيسي

انتخاب الرئيس بيكون على اساس اختيار افضل طريق و الباقي يبقى Backup يعني هش محتاجين خبرة زي ما كانه في الـ DR [Designater router]

* Root switch is switch having least switch ID (MAC address or serial no)
  ↳ بستخدم الـ serial no عشانه يقدروا يتواصلوا في الـ protocol دة فقط
  * الاختيار بيكون على اساس الاقل periority
* periority is 2 byte (16 bit) eig [0 - 65535]
* The default periority is 32,768
* to change periority by this order (config) # spanning-Tree VLAN periority #
* I set the lowest no of periority to the core switch





assume periority of A < B < C

note/ only root switch will send BPDU every 2 sec

---

(3) Electing root port (RP)

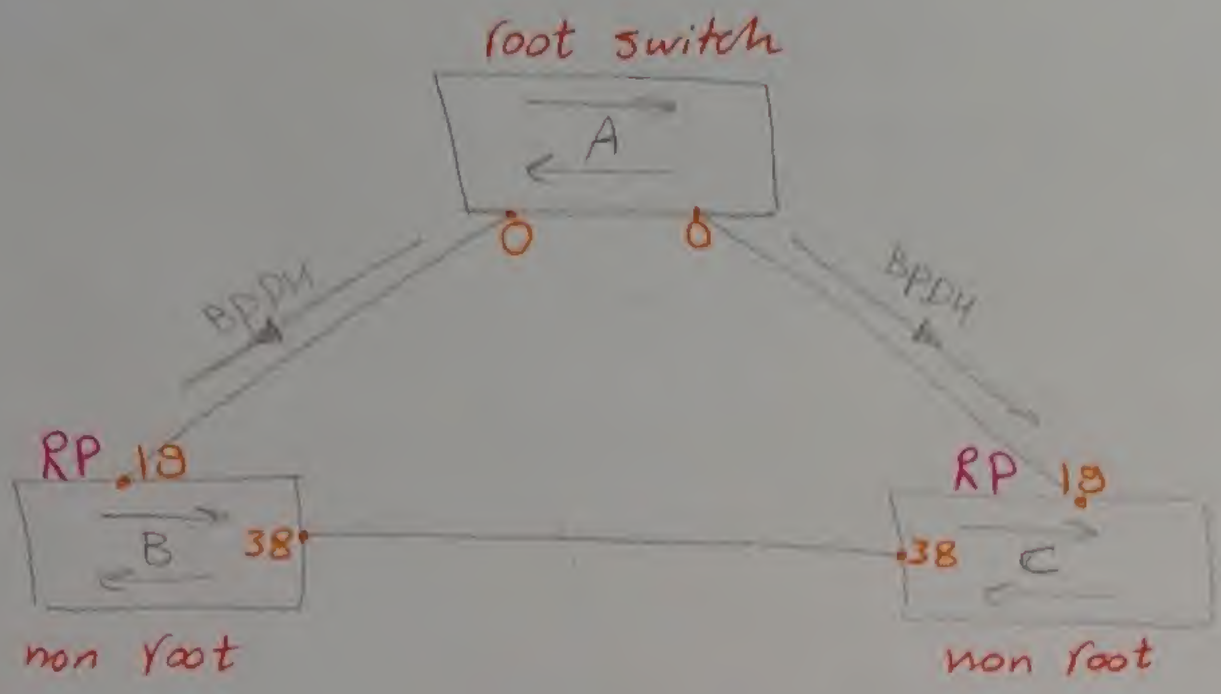
Each non Root switch will choose the best port to reach root switch

RP is :-

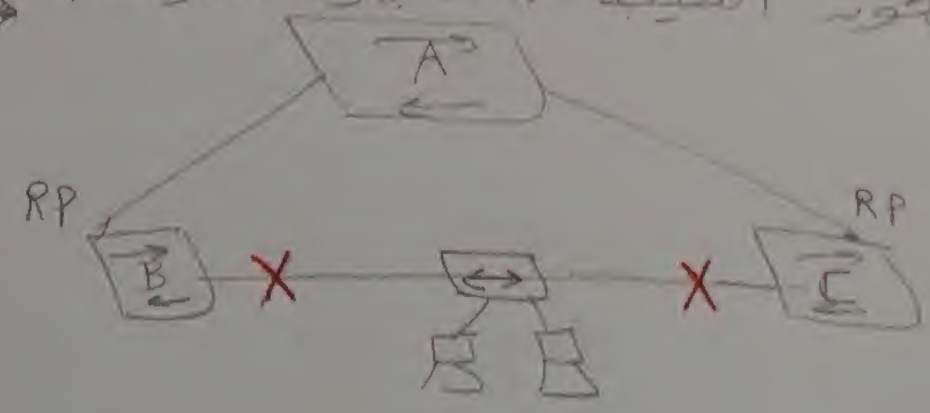
(a) the port having least accumulated path cost Based on BW
(b) port connected to least neighbor switch ID
(c) port connected to least neighbor port ID
اللي port الـ

BW	Cost
10 Mbps	100
100 Mbps	19
1G bps	4
10 G bps	2

* we assume that all links are fast Ethernet [100 Mbps] so the cost = 19



* switch A هيبعت BPDU [0 بـ cost تساوى] لـ switch C و switch C هيشوف الناظر للسرعه 100Mbps والى switch C و هيلاقيها 100 Mbps هيضيف الـ cost الى عندو 19 للـ BPDU frame وهيبعته لـ B switch و بنفس الطريقه switch B هيضيف 19 [هيبقى اللى جاى 38] وهيبعته لـ switch A و switch A لما ترجعله الـ BPDU هيلاقى الـ ID بتاعه جايلو فهيرميها
* هنا طريقه تانى switch A هيبعت الـ BPDU لـ switch B و هيحصل نفس الحكايه
* كل non root switch هيختار The best port من الـ ports بتاعه اللى بتوصله لـ root switch وهيسمى الـ ports دى بالـ Root ports [RP]
وهيسمى الـ ports التانيه بالـ Back up ports
* لاحظ انه مش بيجعلها Back up links عشان ما تقابلش اشكالية انه فى اجهزة متوصله فى الـ Back up link دى لو احنا فصلنا الـ link دى هتفصل 2 ports ← هتكون الشبكه انه الاجهزة المتوصله بالـ



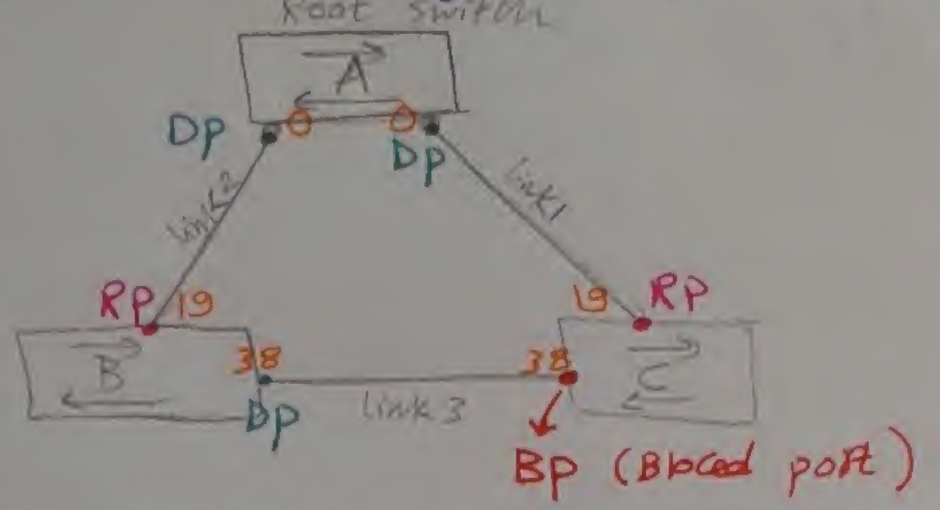
عشان كده هروح لنقطة (4)
وهو انه بدل ما اجعل الطرفين بتاع الـ link يكونوا Blocked ← هجعل واحد بس Blocked

[4] Electing Disignated port [DP]

* it is the best port on each segment [link] that can reach the root switch

DP is

(a) port having least accumolated path cost Based on BW
(b) port connected to least neighbor switch ID
(c) port connected to least neighbor port ID



* في link 1 & 2 هيشوف ال port اللي عليها اقل cost هيخترها كـ (DP)
* في link ده ال 2 ports بتاعة ال link ده ليهم نفس ال cost (38) فهيشوف نقطة (b) فهيلاقي ال switchB له ID اقل وبالتالي هيختار ال port بتاعة switchB ويسميها ال (DP) وبالتالي مش هيبقى الا port واحدة بس هتبقى ناحية switch C ودي بقى هيخليها ال BP [Blocked port]

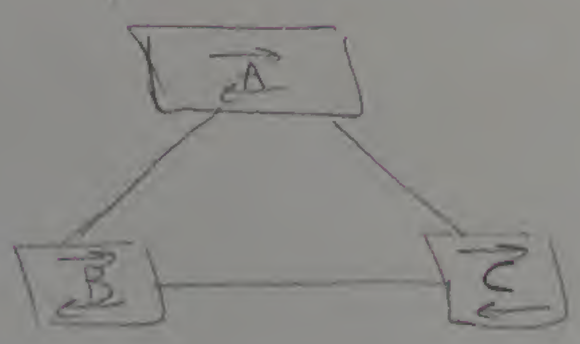
[5] Blocked port (BP)

* ports that are neither RP nor DP

ال port دي بتبقى مقفولة logical يعني اي داتا جاية عليها ⇐ متوقفش drop يعني متعملهاش

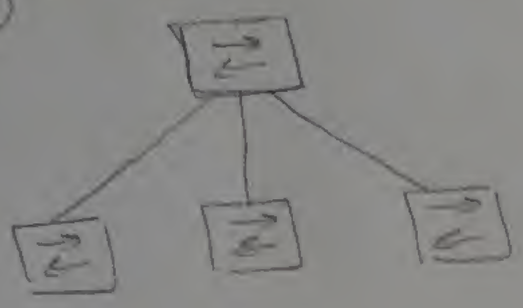
∴ no of BPs = no of links − no of switchs + 1

ex.1



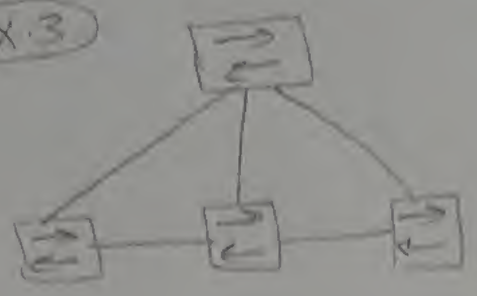
no of BPs = 3 − 3 + 1 = 1

ex.2



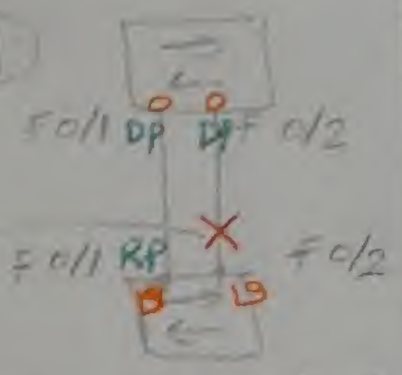
BPs = 3-4+1 = 0

ex.3



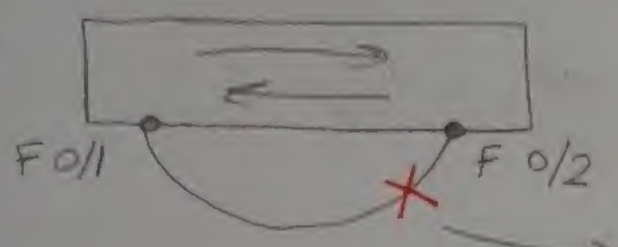
BPs = 5-4+1 = 2

ex.4



BPs = 2-2+1 = 1

ex.5



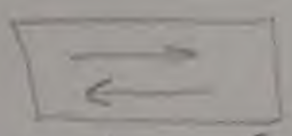
[this port is blocked because it has least ID port]

---

port الـ وجهه نغير الـ ليه شرح

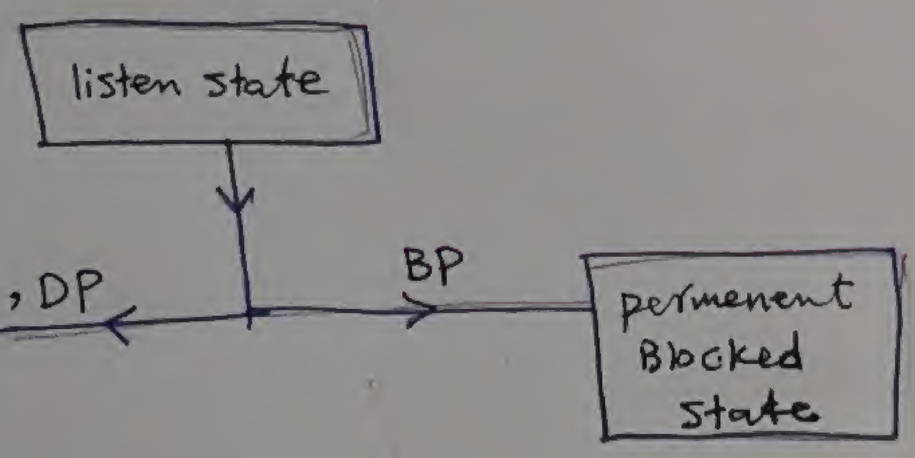
led

Black — Disable state [e.g no cable]



yellow — Temporary Blocked state ← during port load config. < 2 sec

Amber — listen state [15 sec]
* ports start elections [RP > DP > BP]
* ports drop data



* ports drop data
* ports can hear BPDU

it takes 15 sec

* port start forming MAC Table
* port still drops data , led is still amber

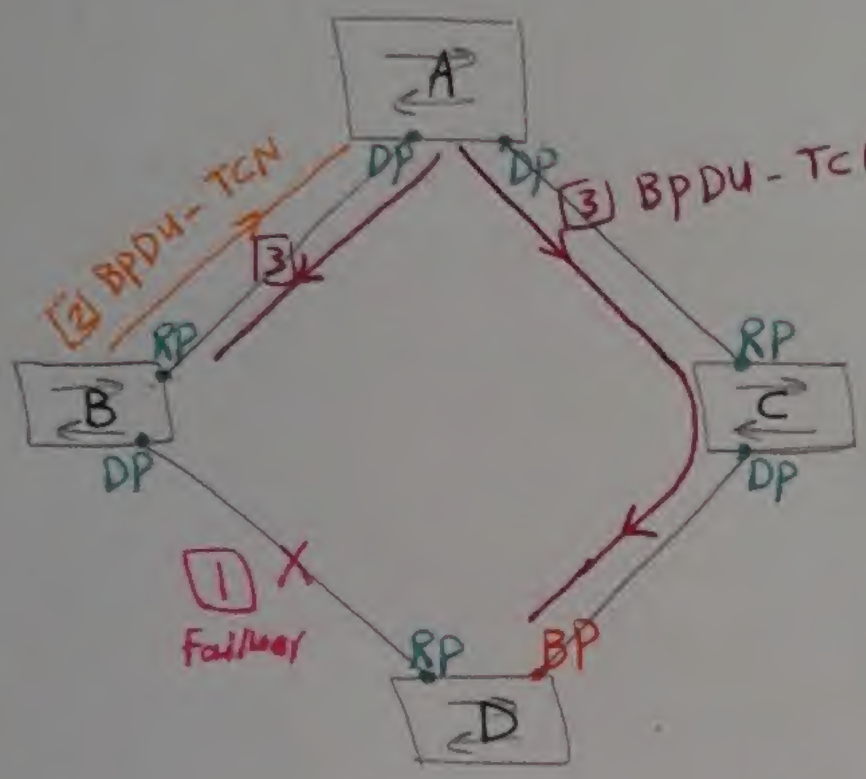
* port starts forwarding
* port is still learning , led is green

Forward state is done at convergence

∴ port either Blocked [standby] or forward [RP, DP]

(III) at change

[1] direct change



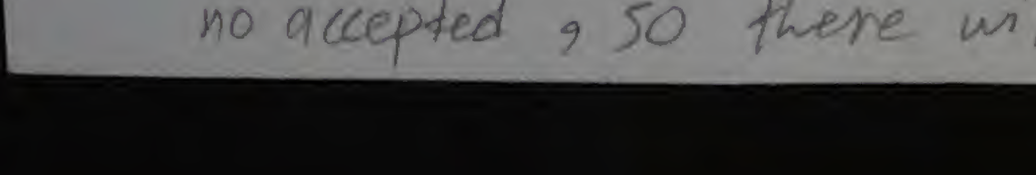
① Failure is exists

② switch that Feels the change will send triggered BpDU - TCN to root switch (topology change Notification)

BpDU-TCN في switch B بيبعت الـ *

③ the root switch [switch A] will send BpDU-TCN to all ports by Flooding

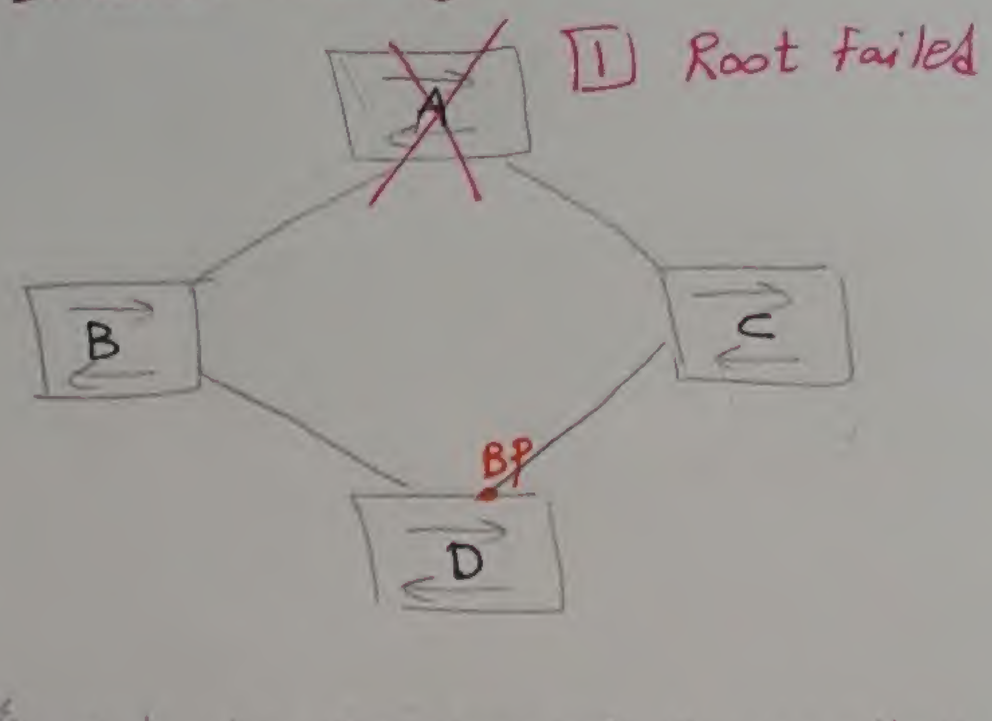
وطبعا كل الـ BPs هتعيد حسابها من اول وجديد



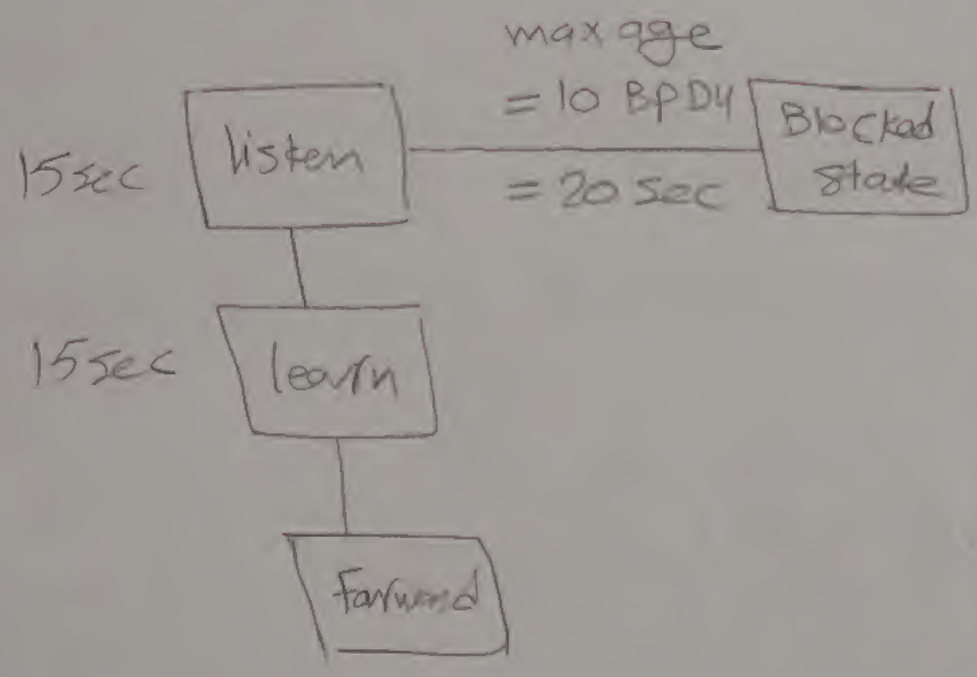
30 sec الحاله دى هتاخد وقت اكتر من الكاميه
Convergence time عشان يوصل لـ

Conv. time = 30 sec

[2] indirect change



فى الحاله دى الـ Blocked port قبل ما هتبدأ تعيد حسابها هتبعت (BpDU msg) زى الـ Hello ١٠ مرات بين الواحدة والتانيه ثانيتين
يعنى الـ switches هتنتظر 2 * 10 = 20 sec
ولو الـ Root switch لم يرد عليها
الـ switches هتعمل انتخابات من الاول



Convergence time = 50 sec

∴ the conv. time between 30 & 50 sec ⟹ that is no accepted , so there will be (RSTP)

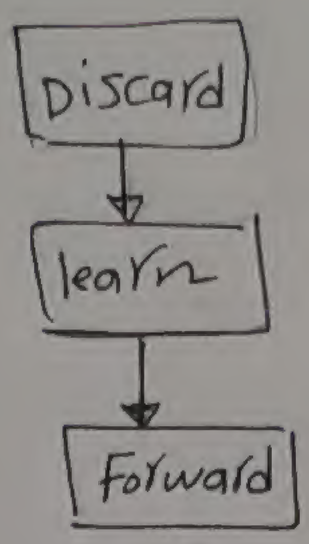
* RSTP [Rapid STP] IEEE 802.1 W

it was [STP + cisco Enhancement = ESTP] cisco خاص بشركة
standard_T طلع IEEE من

First Enhancement / they grouped disable & blocked & listen states
in to one state called Discard state

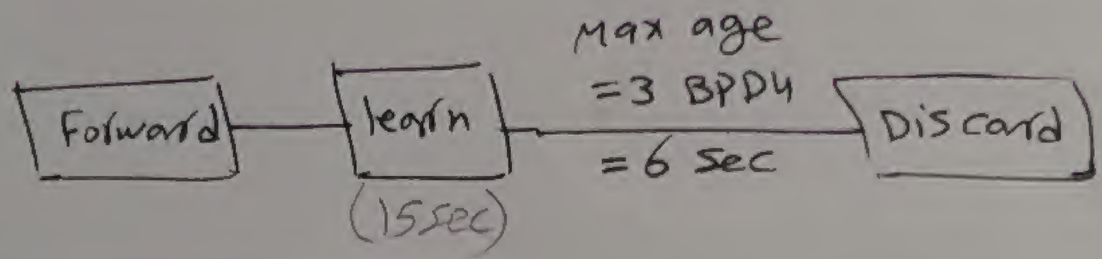
① in direct change

15sec الى 30sec من انا حسبت بكره



i Conv. time = 15 sec

② in Indirect change



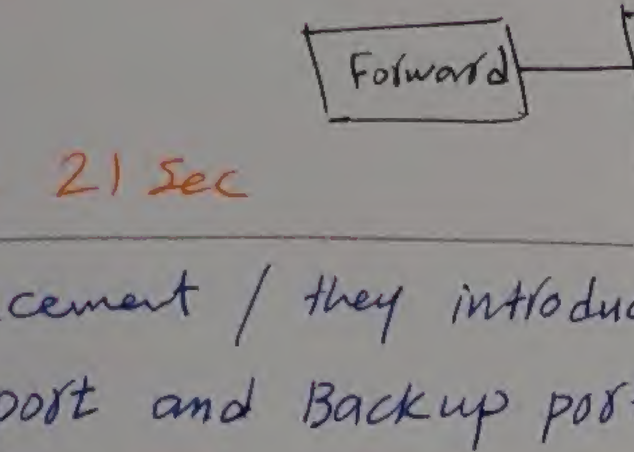
Conv. time = 21 sec

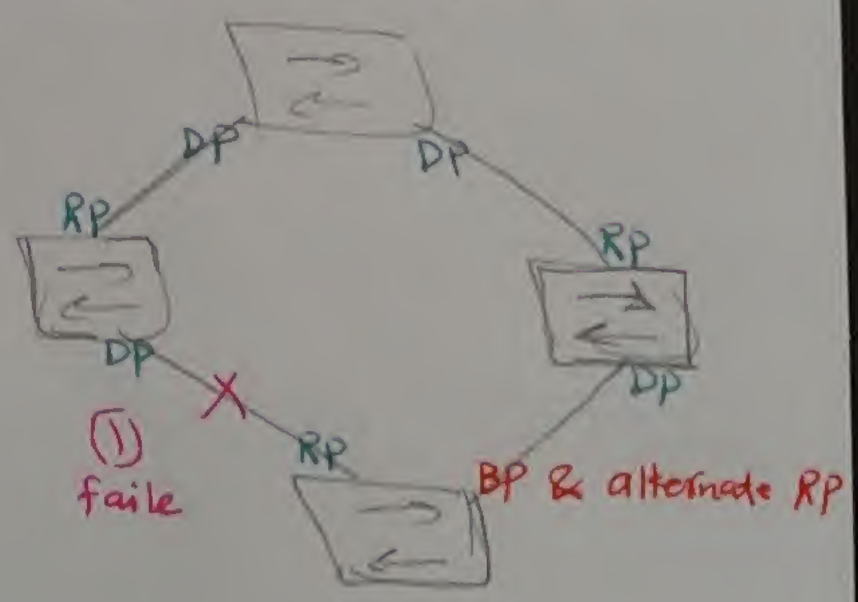
---

second Enhancement / they introduce extra elections [new port rules]
→ alternate port and Backup port for each [RP & DP]

① Direct change

بمجرد ما يحصل Falure ع الـ BP تروح محوله
RP الى [2sec من اقل ف] Immediatly نفسها





conv. time < 2 sec

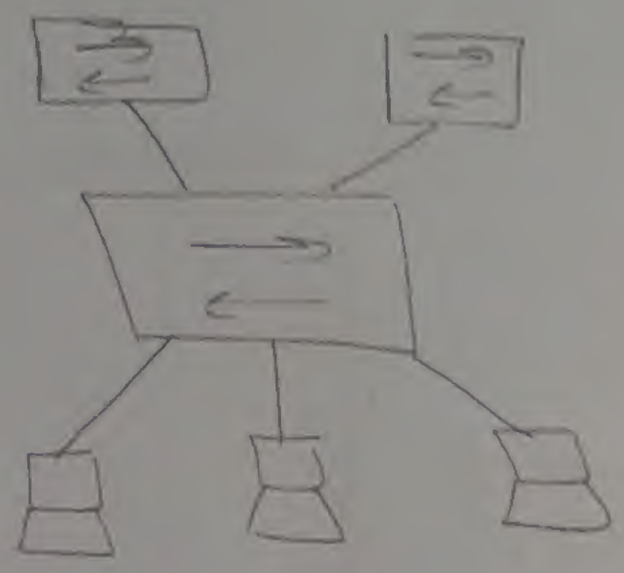
---

② indirect change

في الحاله دي لازم يتم انتخابات من اول وجديد وعشان كده كان الحل انهم
يعملوا اوى بال Root switch في انه متعملش من power supply كده كده

third Enhancement / they introduce a concept called port fast

port fast / port that jump to forward state immediatly , it should be used with ports connected to PCs (DTEs)



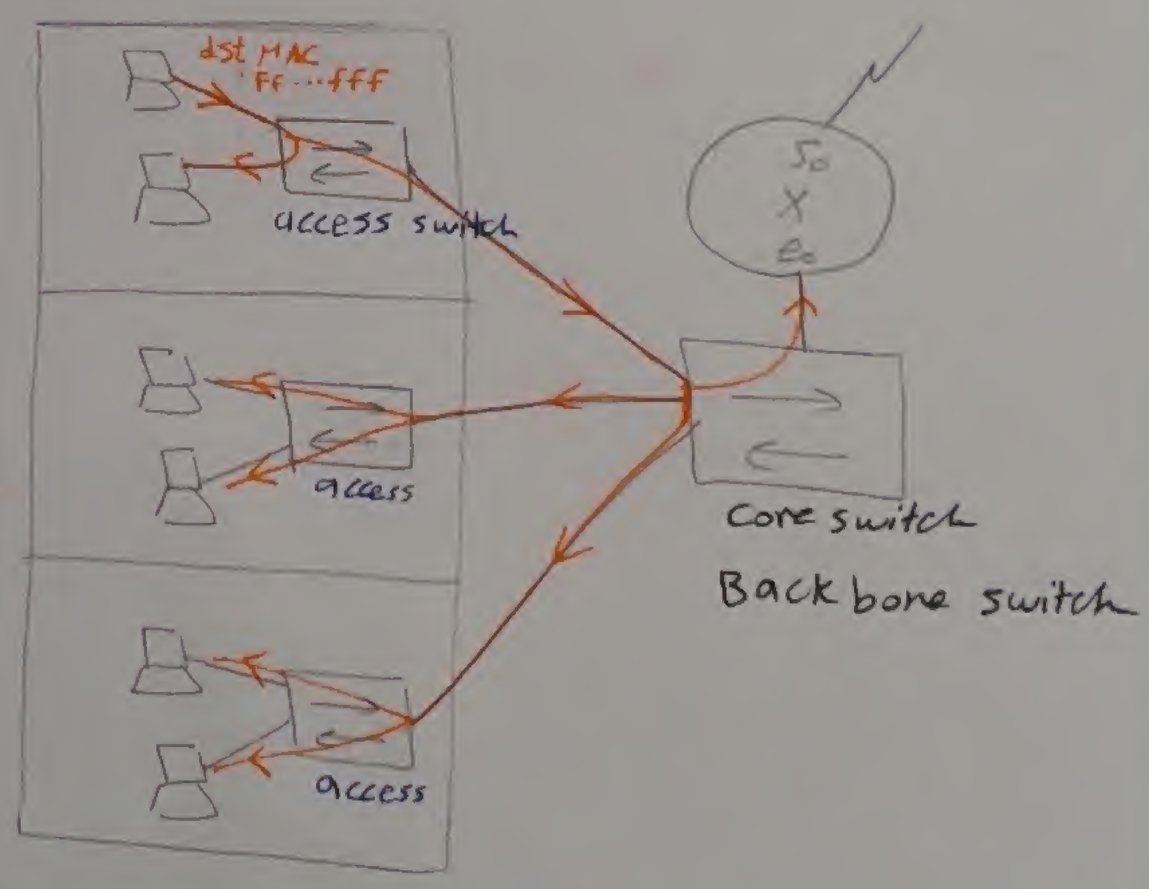
الخاصيه دى عشان ال PC لما تعمل Restart او تعمل
مينتظرش 50 sec عشان لما تيجى
بال Network و اول ما ال PC
يعمل restart ← ال port اللى متوصل
بيه هى حس بيه ويوصله
على طول بال Network

(config-If) # spanning-Tree port Fast

The main problem here is Flooding

Food occures when → Broadcast
→ Mullicast
→ unknown unicast

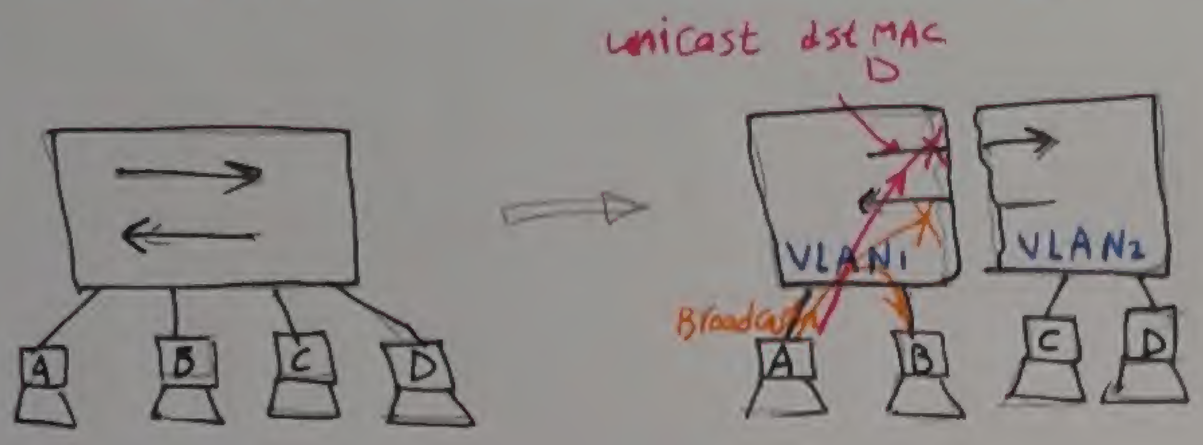
عليه ال Flood بتخنق الشبكه جدا



The solution is using VLAN [vertual LAN]

VLAN : vertual LAN [It works as software Isolation]

* we devide one physical switch to more than one vertual switch
* you can make every port on a switch as VLAN
* max number of VLANs per switch = 4096 (12 bit)
* the use of VLANs is to decrease flooding



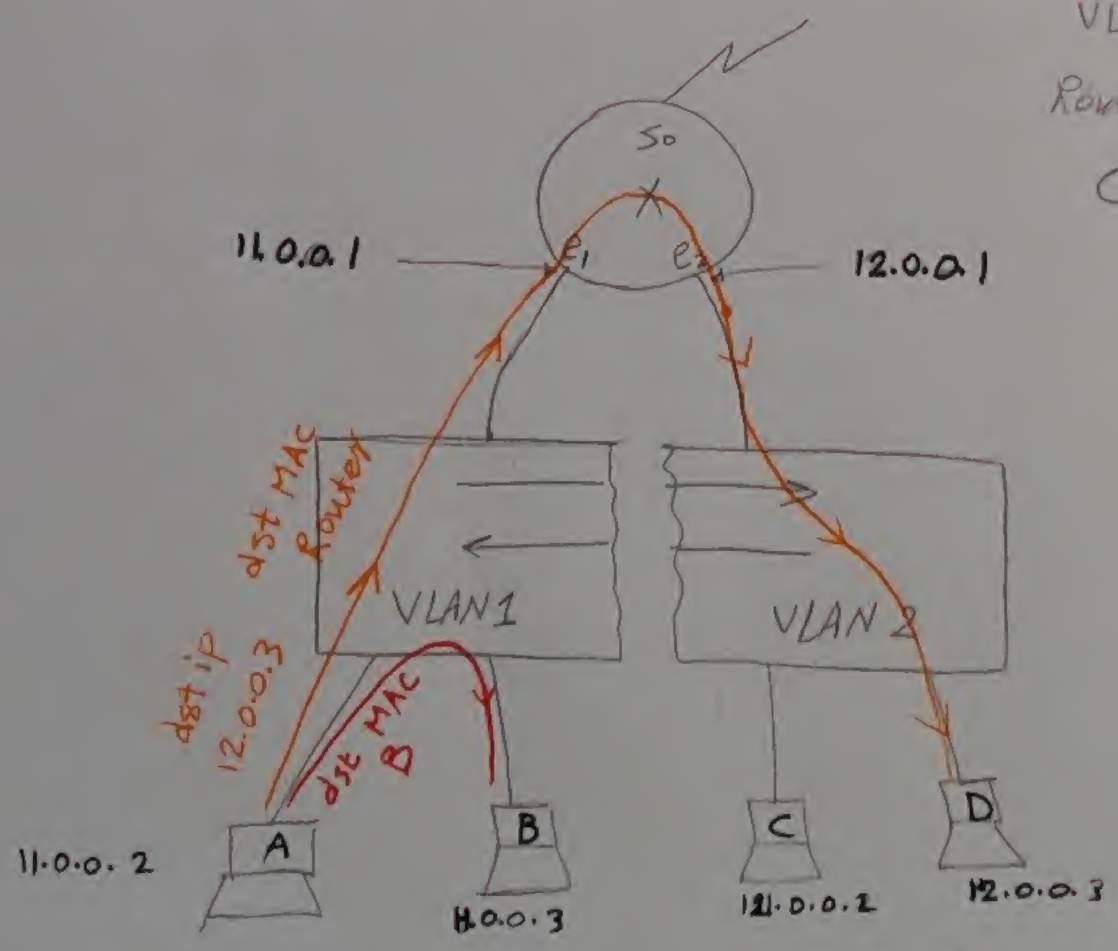
مفيش Broadcast هيمر من VLAN1 الى VLAN2 وده كويس
بس المشكله انه هيوقع الداتا
اللى جايه unicast من
VLAN الى VLAN2 وده مشكله عشان كنا هنفكر فى استخدام Router

→ each VLAN is a broadcast domain

* Inter VLAN Routing الحل فى

(1) Traditional solution (5% of usage)

* هنا بنستخدم Router وبنعتمد على مزايا ه انه لا يبعت broadcast ولا بيعمل Flooding
* ملحوظه / اجبل لكل VLAN ← Subnet
*each VLAN has a unique subnet



* الشكله هنا انى هحتاج لكل VLAN كابل + Interface خاصه على الـ Router والـ Interface دة بيبقى تالى اوى

* ملحوظه/ الـ PC مش بيفهم يعنى ايه VLAN لكنه بيفهم Subnets

[2] Router on a stick (75% of usage)

port - هنا مستخدم واحدة بين ال switch واكتر اوصل لأي VLAN عن طريقه

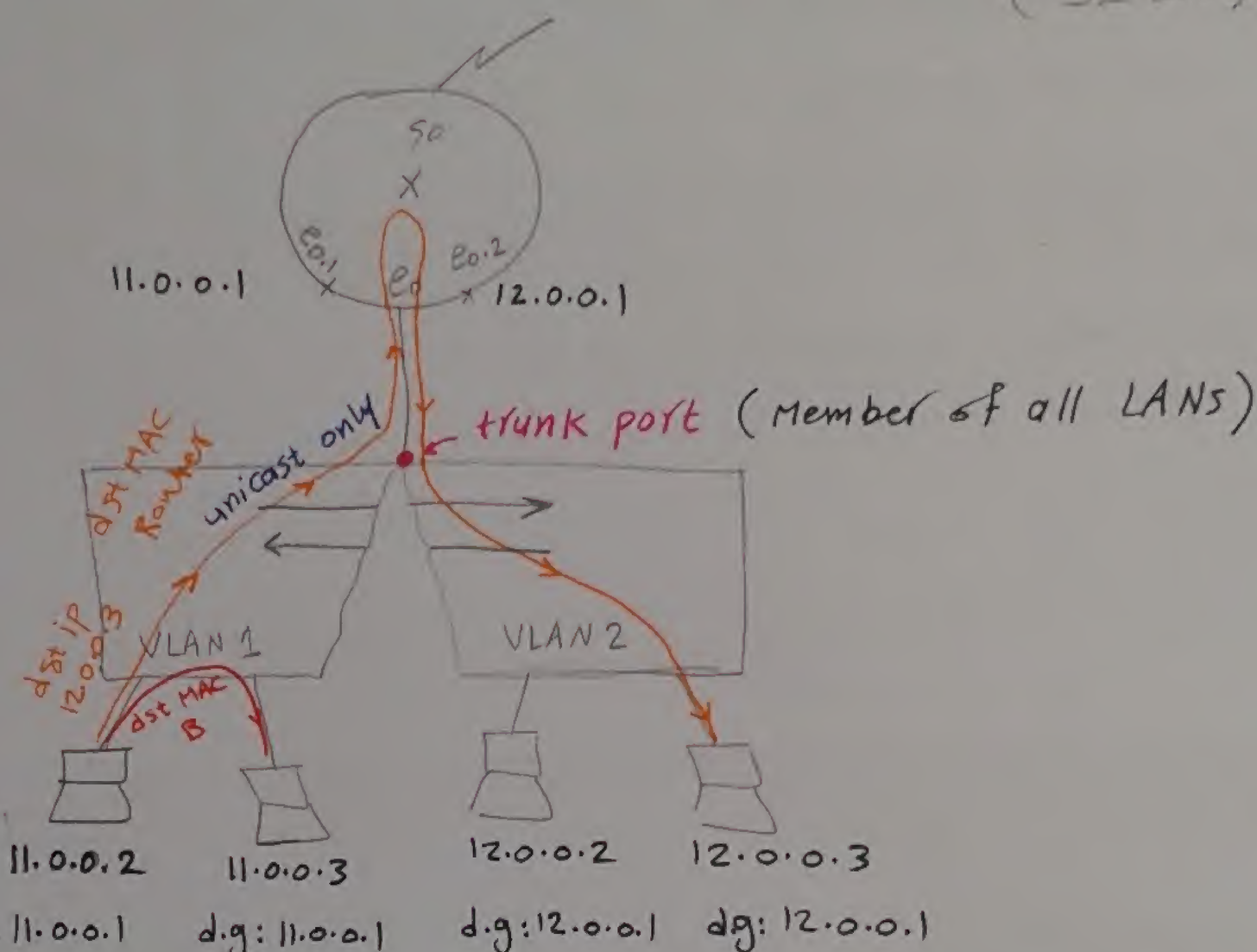
ال port دي واوصل ال Interface دي ← واحدة بين ال Router

[trunk port]

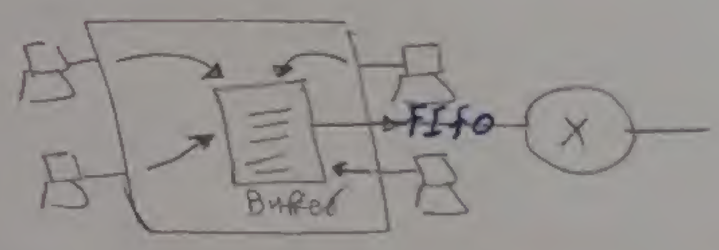
* اقسم ال Interface اللي على ال Router الى virtual subinterfaces

* اكتر اقسم ال Interface الواحدة على ال Router الى virtual subinterfaces 4b XXXXXXXX XX

(32 bit)



* the trunk port must have very High B.W ⟹ مثلا ~ كل ال PCs بتستخدم في ال unicast



Disadvantage

1- congistion

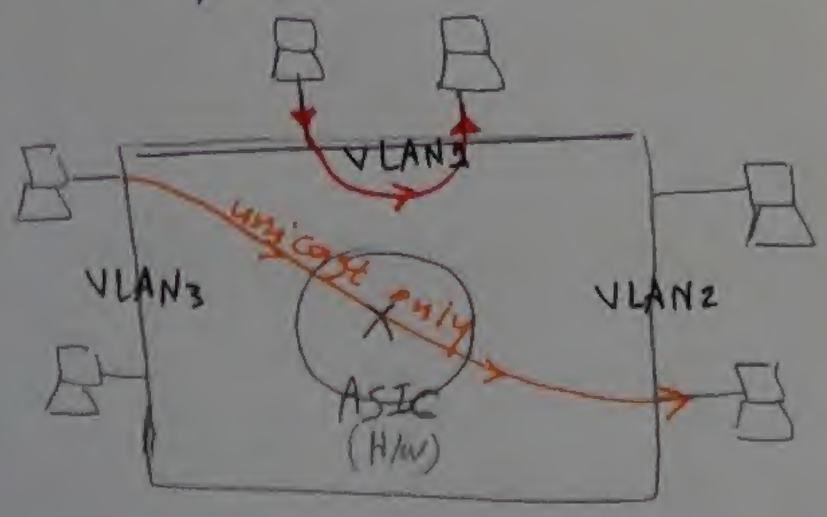
2- Single point of failure (i.e) If the trunk port is cut, the all Network will be fallen

3- S/W Based because of Router

---

[3] Multilayer switch (20% of usage)

→ layer 3 switch



* هو في الاساس switch كل الـ ports بتاعته base the same Comm. Technology

* بيحل كل الـ ٢ مشاكل اللي فاتو الكمبيوتر

بس very Expensive اه

* The configuration for [2] Router on a stick

General

```
(config) # int e0
(config-if)# no shut down
(config-if) # no ip address
```

For e0.1

```
(config)# int e0.1
(config-subif) # encapsulation dot1q 1   ← VLAN no
(config-subif) # ip address 11.0.0.1 255.255.255.0
```

For e0.2

```
(config)# int e0.2
(config-subif) # encapsulation dot1q 2
(config-subif) # ip address 12.0.0.1 255.255.255.0
```

e0.1
e0.2
e0.3
:
e0.N

← Virtual interfaces عدد ال حسب على تاتى تكون تقدر

---

* Switch port types

[1] access port

* it is a port that is a member in only one VLAN
* it is a port that is connected from switch to PC

to configure one port	to configure range of ports
(config) # interface F (fast Ethernet) 0/3 (port no) (config-if) # switchport mode access	(config) # interface range f 0/3-15, 19 From 3 to 15 and 19 (config-if) switch port mode access

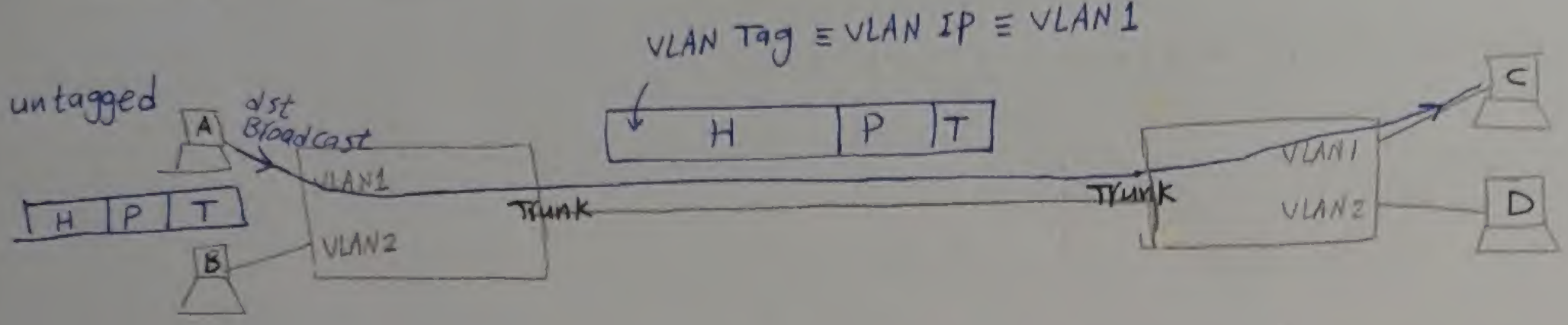
ملحوظه / لما تقول لل port انت access ← هيعتبر نفسه من (Native LAN) default LAN
الى هو VLAN1 و تقدر تغيره بال Configuration

[2] Trunk port

* it is a port that is a member of all VLANS by default
* That port is a port connected from switch to a router or to another switch

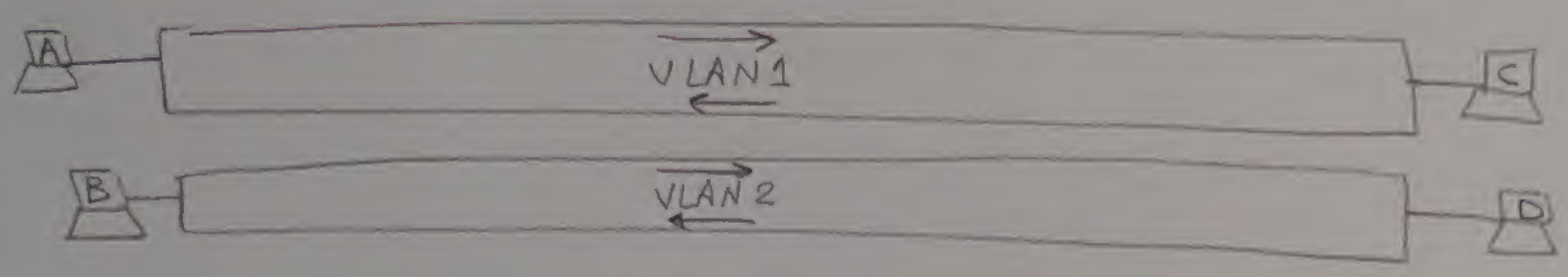
```
(Config) # int f 0/24
(Config-If) # switchport mode trunk
```

Trunk of switch to switch



ال Trunk switch بيضيف ال Tag للـ frame عشان يقدر يعمل Broadcast على نفس VLAN بس متوصله بـ switch مختلف وال Tag دة بيبقى فيه اسم ال VLAN ⇒ VLAN ID

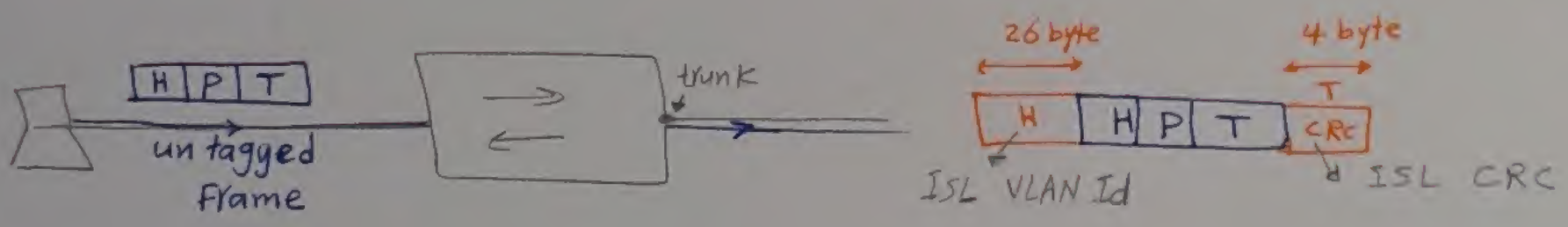
∞ VLAN Can span Multiple switches



---

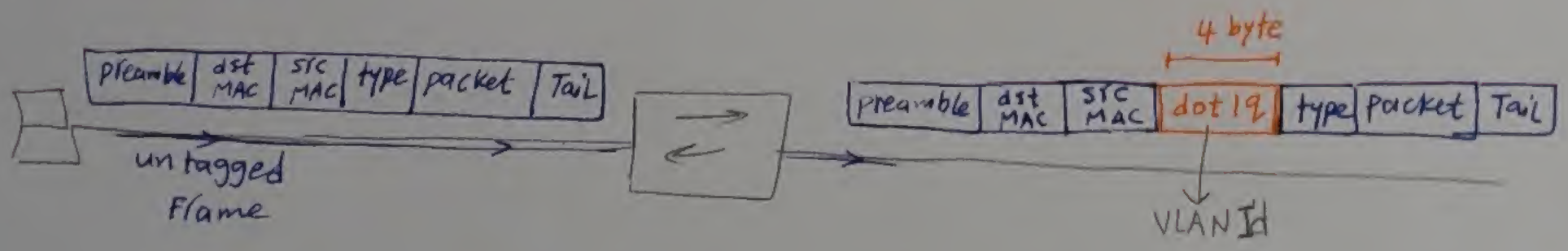
* Tagged types

[1] ISL [inter switch link] by Cisco



تكنه فشل لانك اضفت 30byte ⇐ كتير اوى

[2] IEEE 802.1q



VLAN configuration

[1] create VLAN database : VLAN.date

(config)# VLAN VLAN #

(config-VLAN)# Name VLAN name → option

to show VLANS → ## show VLAN

you can configure all data base on one switch and spann them

EX

(config)# VLAN 2
(config-VLAN)# name HR
(config)# VLAN 3
(config-VLAN)# sales
⋮

number #	Name
VLAN 1	default
VLAN 2	HR
VLAN 3	sales

[2] activate VLAN on switch port

(config)# inerface F 0/4

(config-if)# switchport mode access → by defaut port 0/4 will be in VLAN 1 (native VLAN)

→ to change the port 0/4 to a specific VLAN, you can type

(config-if)# switchport mode access VLAN #

[3] configure Trunking & Tagging

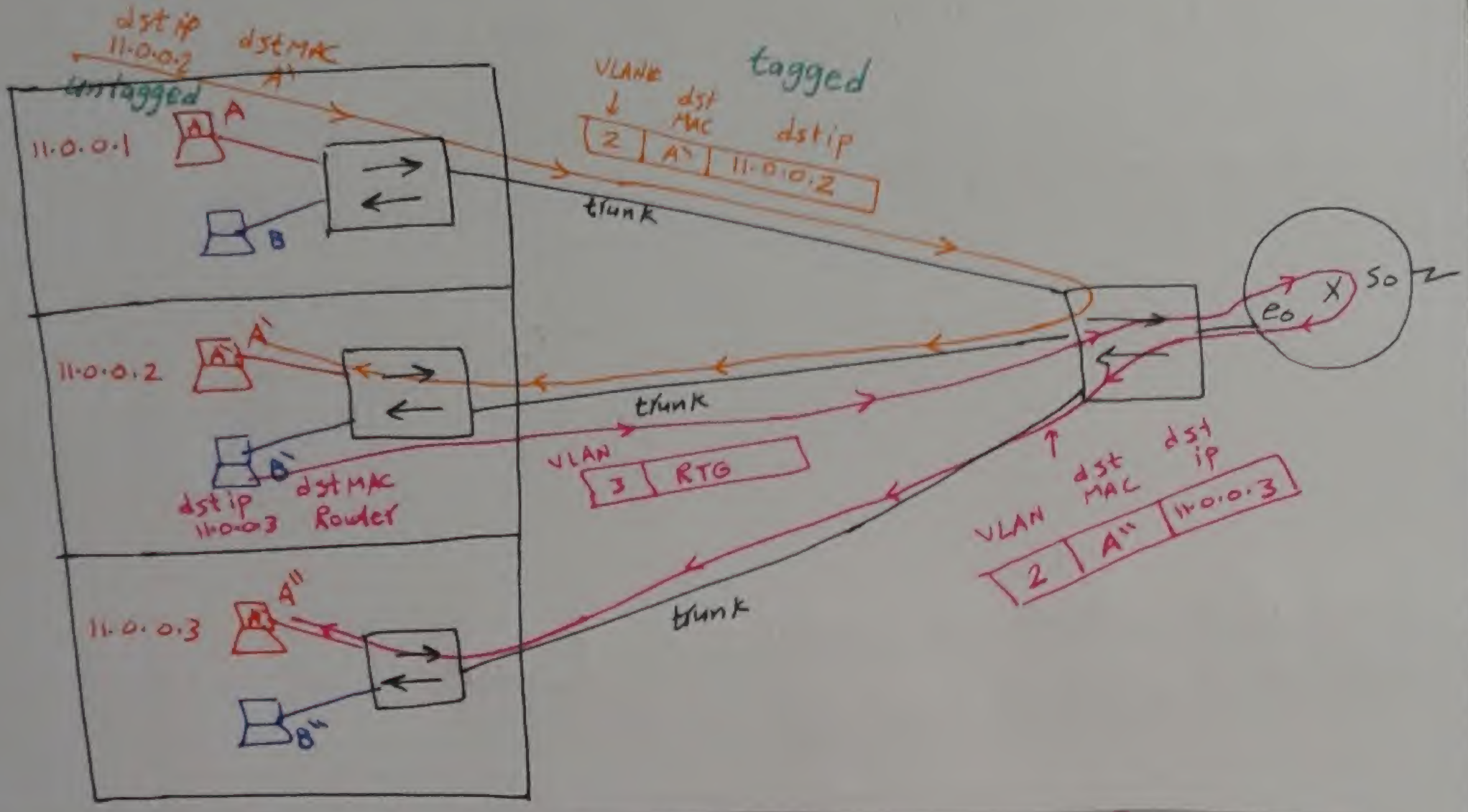
(config)# int f 0/24

(config-if)# switchport mode trunk

→ to choose the tag type [ISL or dot1q], you can type

(config-if) switch port trunk encapsulation { ISL | dot1q } (or)
tag

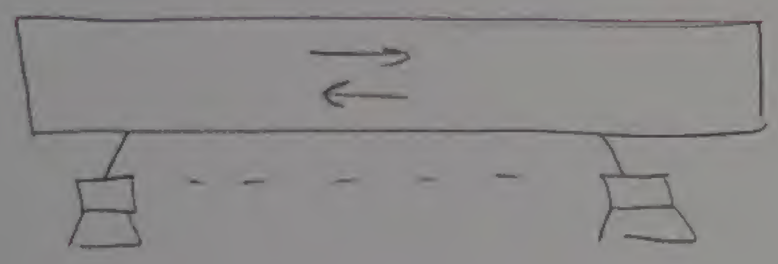
note/ this order is not written in some switchs like [catlayest]
because the default tag in it is dot1q



---

* (config-If) switch port mode access VLAN ___ # الامر دة عشان تحدد VLAN معينه الـ port

→ Static VLAN membership (98% of usage)
[port Based VLAN]

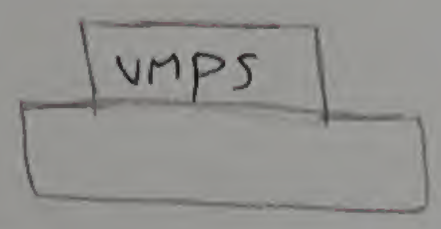


وهنا انت بتغير الـ default VLAN بايدك من Native VLAN (VLAN1) الى رقم الـ VLAN اللى انت عايزها

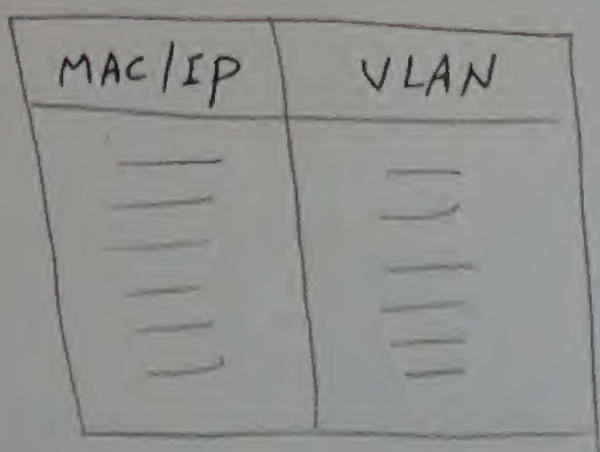
→ Dynamic VLAN membership (2% of usage)
details in CCIE Course
[MAC/IP based VLAN]

[VLAN membership policy server] VMPS اسمه server

* فى الاول انت بتجيب كل MAC/IP لكل جهاز والـ VLAN اللى بيستخدمو و بتكتب فيه جدول كامل عند



* كل ما DTE = connect على الـ Switch و الـ Switch صيسأل الـ Server [ايه هو الـ VLAN اللى مشترك فيه جهاز الـ MAC او IP بتاعه xxxx]

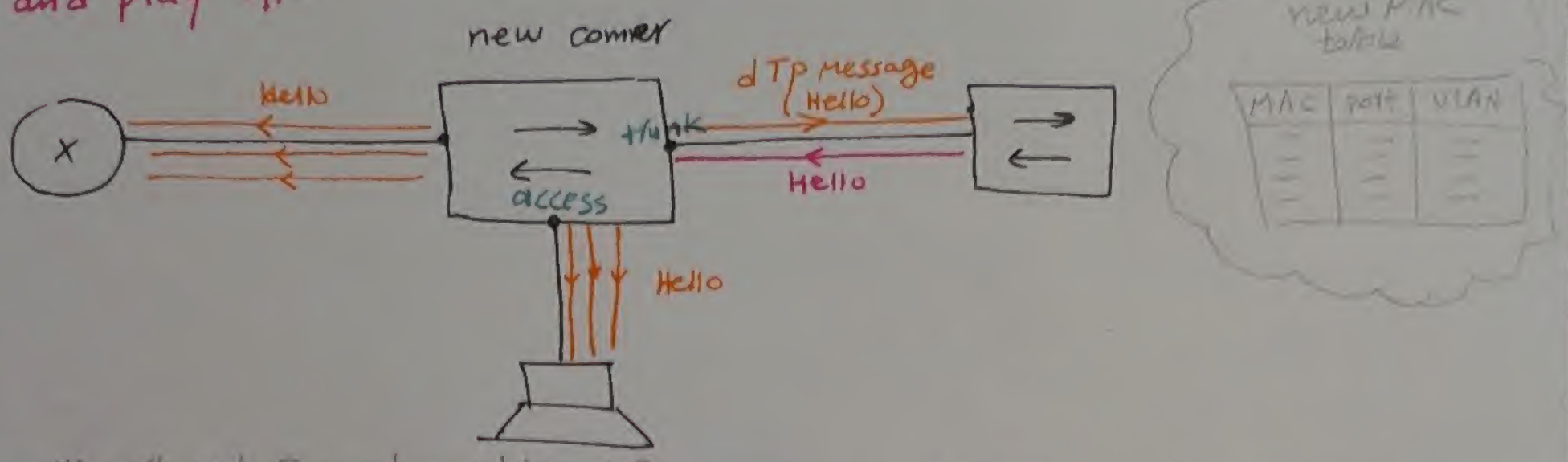


* ودة بيوفر لنا انه الـ port مش شرط تكون ثابته فى مكان معين

⟹ this Dynamic membership support security and Mobility

DTP : Dynamic Trunk protocol → for cisco switchs only

* it's work is to negotiate whether port should be access or trunk
* it is plug and play type



(config-If) # switchport mode [access | Trunk | dynamic] ← DTP

* اول ما الـ switch الجديد يتوصله power هيرسل dtp msg (Hello) على كل الـ ports
* لو الـ switch التانى هيبعت Dtp msg ، و يقوم الـ switch الجديد بـ configure الـ port دى على انها [Trunk port] ← Dinamically
* لو الـ switch التانى مش هيبعت DTP msg و هيـ configure الـ port دى PC على انها access port

* المشكلة الوحيدة هنا من الـ Router فى انه مش هيفهم DTP msg وبالتالى مش هيبعت الـ switch هيعتبر الـ port ← access وهى فى الحقيقة trunk
⇐ الحل انى اروح على كل الـ ports المتوصله بالـ Routers و اعملهم config.
(Config-if) switchport mode trunk

---

* Managing switch Remotely

(config) # line VTY 0 15 ← يقدر 16 واحد يعملوا Telnet لـ switch فى نفس الوقت
(config-line) #password cisco
(config-line) # login

(config) # interface VLAN #
(config-if) # ip address IP Mask ← هنا بنعرف الـ switch هيتعرف بـ IP ايه و هيتعامل بـ Telnet ازاى
(config-if) # no shutdown
(config) # ip default gateway ipof router ← هنا بنقول الراوتر هيوصل الـ switch ازاى

VTP 33 min lec 18

* VTP [VLAN Trunking protocol] for cisco switchs only

- it is responsible for synchorization VLAN Database

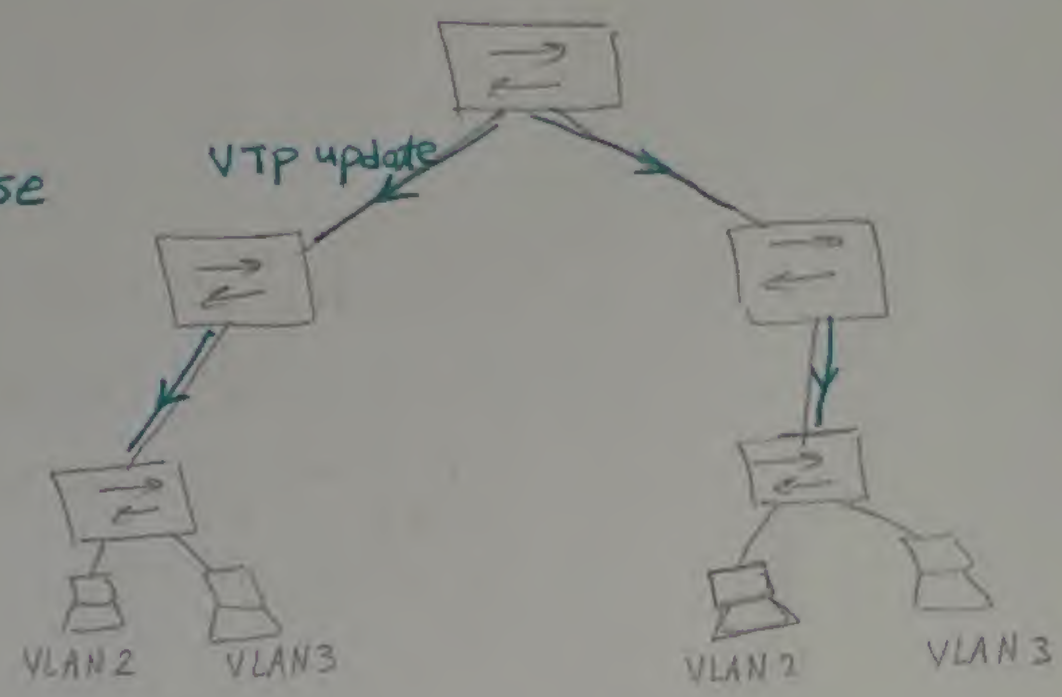
* you can configure any switch [it is not condition the root switch] with VLAN.dat . and this switch will propogate this (VLAN.dat) to all switchs by flooding

note
* If switch doesnot know VLAN , it will drop data
* " " " " MAC address , it will Flood data

* VTP conditions for switches that accept the VLAN.dat

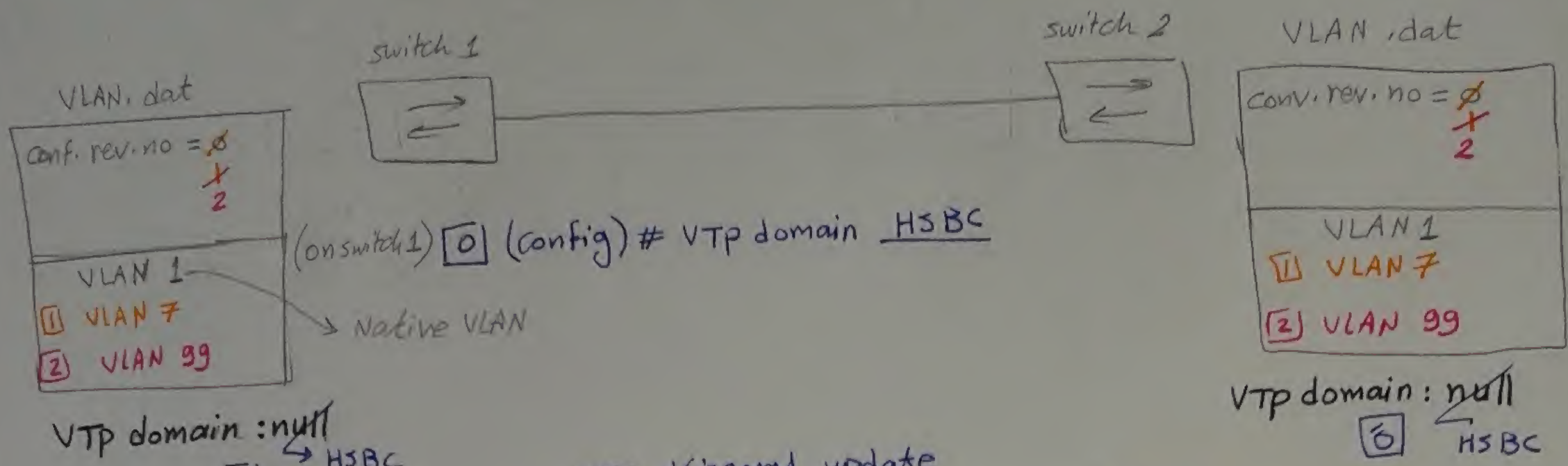
1- Link between switches should be trunk
2- Same VTP domain (AS)

VTp update contains VLAN database



VTP operation :-

* Configuration revision number : is a number that represents the changes [update العدد] that happen in VLAN.dat
* when the switch is new to a network , then the conf. rev. no = 0
* لاحظ انك تقدر تعمل configure لـ switch وهو بعيد عن الـ VTP update باقي السويتشات
* the VTP domain name is by default (null) untill you configure it with specific name
* the default of all switchs is server untill you configure it as Transparent or Clinet → it will be explained next
* the Domain Name is case sensitive (ei) HSBC is one domain name & hsbc is another domain name



(on switch 1) [0] (config) # VTP domain HSBC

→ Native VLAN

VTP triggered update

" VTP domain HSBC "

(on switch 1) [1] (config) # VLAN 7

VTP triggered update

VLAN. dat	Revesion no	VTp domain
1 7	1	HSBC

(on switch 2) [2] (config) # VLAN 99

VTP triggered update

VTP domain	revision no	VLAN. dat
HSBC	2	1 7 99

* If you want to change the Domain name to (XYZ), then you have to configure this command [(config) # VTP domain XYZ] in all switches & every switch at atime (واحد واحد switch لأ)

* بعد ما تـ configure VLAN 7 على switch 1 & switch 1 هيبعت Step 1 : Vtp Higgered update لكل الـ switches اللي حوليه عن طريق Flooding [في حالتنا بس switch2]

* switch2 & switch2 هيبص على الـ revision number اللي موجودة في الـ update ويقارنه بالـ revision no اللي عنده & لو وجد الـ revision no اللي في الـ update أكبر منه اللي عنده هيعرف ان الـ VLAN.dat اللي عنده بقت Expired وهيحذفها كامله ويضع مكانها الـ VLAN.dat اللي لسه جايه في الـ VTp triggered update & وفي نفس الوقت هيزود الـ revision no بتاعه بقيمة 1

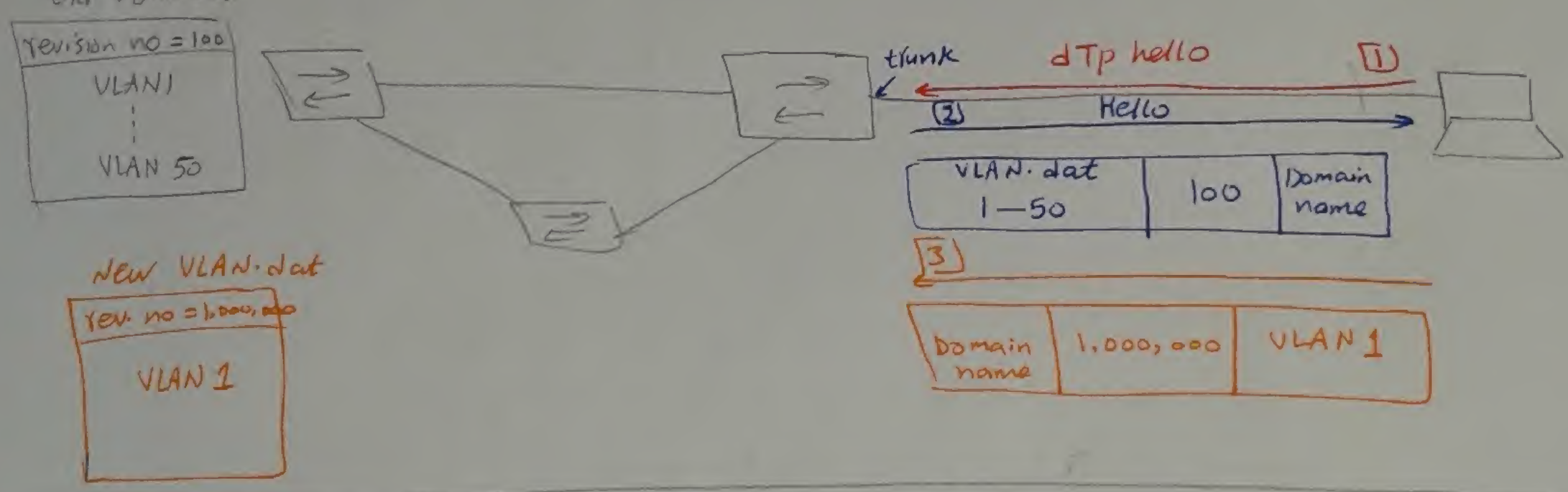
* Step 2 زي Step 1 بس الفرق الوحيد انه الـ config. كان على switch2

* في حاله اختلافه ال Network

1. ال pc هيبعت dTp Hello على ال switch
2. ال switch هيعرف ان ال pc دة عبارة عن switch [طالما شاف ال dTpHello] وهيغير نوع ال port المتوصله بال pc من access الى Trunk وهيبعت VTP update لل pc
3. ال pc هيبعت لل switch ← VTP update بنفس ال Domain name وهيغير ال VLAN.dat وهيكتب في ال revision no رقم كبير اوى (1,000,000) عشان
4. اول ما ال switch هيشوف ال revision no اللى فيه جايه اكبر منه اللى عنده ما هيحذف كل ال VLAN.dat اللى عنده و هيضع بدلها الجديد [الخبرة] وبكدة اى Data جايه لـ VLAN معينة ، ال switch مش هيعرفها و هيـ drop الـ Data

⟸ كانه العمل في ال command دة عشان يزود ال security ما ولاحظ انه الامر دة لازم تكتبه لكل switch على حده

(config)# VTP password password (option)



---

* (Config)# VTP version {1 | 2} ⟹ by default version 1

Note/ Verion 1 & version 2 are incompatible ، (ei) all switchs in a single Domain must have the same version

* (config)# VTP mode { server | Client | Transparent }

⟹ by default server

⟸ # show VTP status

There are three modes that switch can take place

1. server
   * configuration VLAN.dat manually
   * propagate VLAN
2. Transparent
   * config. VLAN.dat manually
   * by pass VTp updat only
3. Client
   * does not accept any manuall VLAN.dat configuration
   * accept VLAN.dat From VTp update only

---

* wifi (wireless lAN)

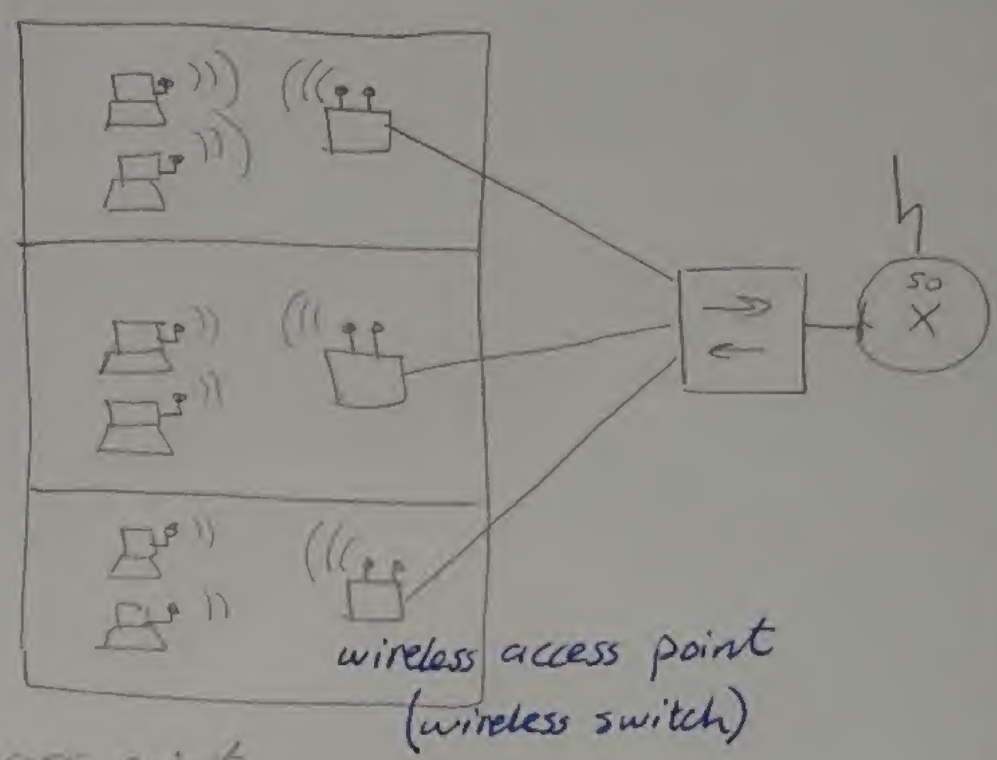
* the used communication Technology is

  CSMA/CA

  [Carrier sense multiple Access / Collision Avaidance]

* the used antenna type is

  Omnidirectional antenna



CSMA/CA ⇒ If 3 PCs use the same access point
it makes one PC send and the other PCs are recaiving
or waiting some time untill it finish.

فكره التخصيص في نفس ال Access point مع العلم انه بتقلل السرعه و كمان
بتشتغل Half duplex

Note / لنفترض ان ال Access point بيعطي سرعه 100 Mbps

السرعه اللي ال PC بيأخدها بتعتمد على المسافه بينه وبين ال Accesspoint
يعني لو ال PC جنب ال Ap مباشرة هتبقى سرعته 100 Mbps
وكل ما هتبعد ال PC عن ال AP، كل ما السرعه هتقل لحد
ما توصل لـ NO signal

Accesspoint

* there are two bands used for wifi 2.4 GHz & 5 GHz
* 5 GHz is not used in Egypt [in America and canada only]

BW = 83.5 MHz & Channel width = 5 MHz/ch

∴ no of Channels = $\frac{83.5 \text{ MHz}}{5 \text{ MHz/ch}} \simeq 16$ ch.

no of ch after Gaurds = 14 ch

---

[2] Wifi standards : IEEE 802.11

(A) IEEE 802.11 B (standard B)

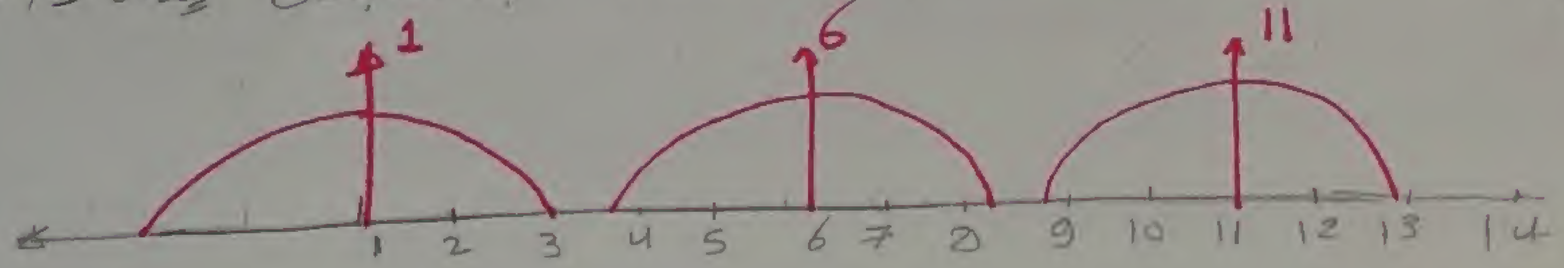
Band : 2.4 GHz

# of Channels : 14 chs (3 non overlapping area (e.g) 3 only are available for usage)

Speed : 11 Mbps

Tx Tequnice : DSSS (Direct sequance spread spectrum)

* لكن لا يكون معنا overlapping يعني الـ Frequencies المستخدمه تكون بعيده عن بعض على 5 chs



1 - 6 - 11 ← more usable
2 - 7 - 12
3 - 8 - 13

(B) IEEE 802.11 G (standard G) [used in Homes]

Band : 2.4 GHz

# of chs : 14 chs (3 non overlapping area)

Speed : 54 Mbps

Tx Technice : OFDM (orthogonal Frequency Devision multiplixing)
& DSSS → for standard B

∴ note / standard G is compatible with standard B

ⓒ IEEE 802.11 n (standard N) (الاحدث في السوق)

Band : 2.4 GHZ

# of chs : 14 (3 non overlapping area)

Speed : 108 Mbps ⟶ 384 Mbps

Tx Tequnice : MIMO

ⓓ IEEE 802.11 a (standard A) used in America & CAnada only

Band : 5 GHZ

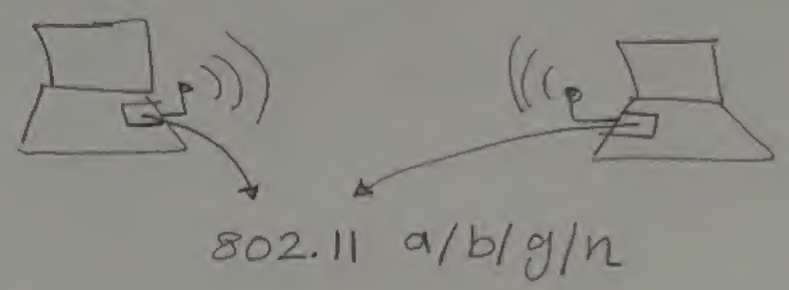
no of chs : 60 (12 non overlapping area)

speed : 54 Mbps

---

* Wifi design

[1] Ad hoc Mode: (point to point) ⇒ اتصال لحظي



non service set

* Access point is called Service set also
wireless عدة الـ

"IBSS" independent Basic service set

---

[2] Infrastructure Mode: (شبكة ثابتة مثلاً في كافيه او البيت)

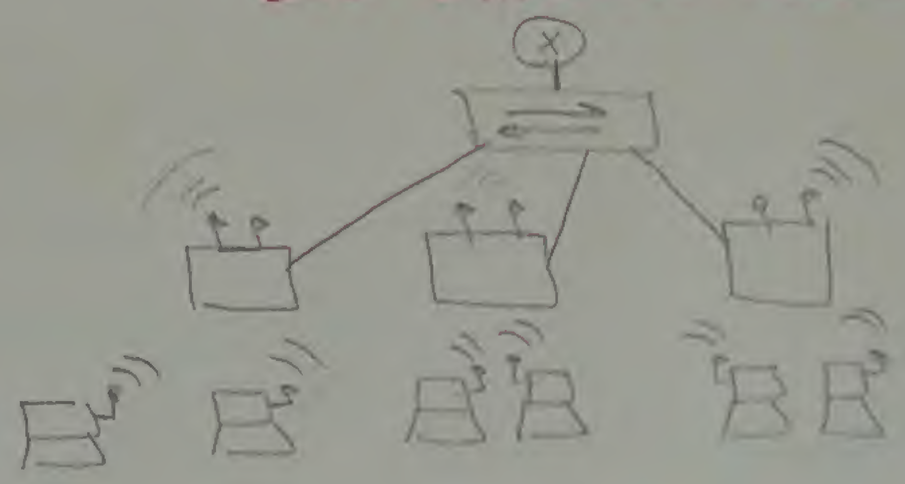
Star topology

only one access point

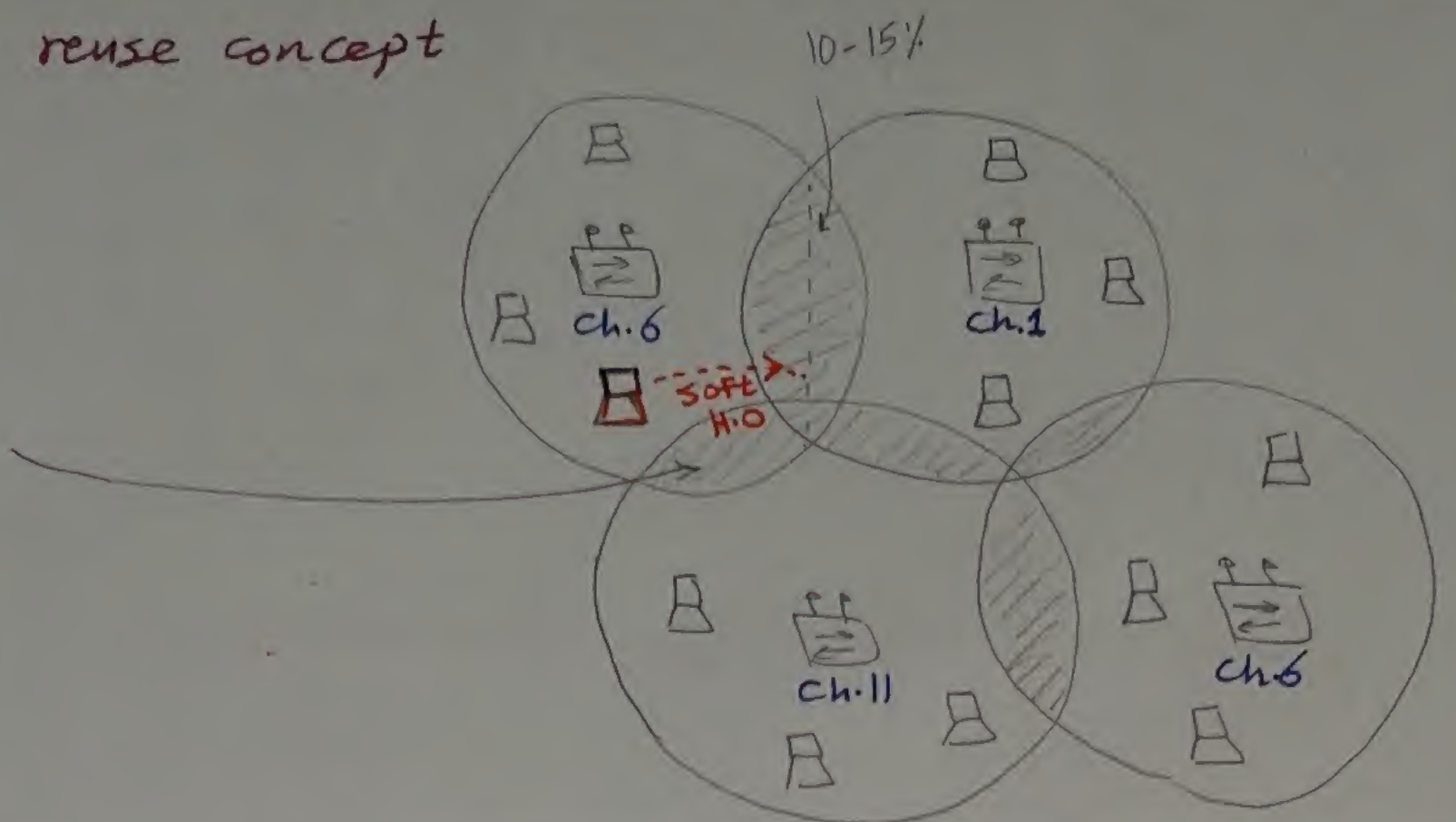
"BSS" Basic service set

more than one access point

"ESS" Extended service set



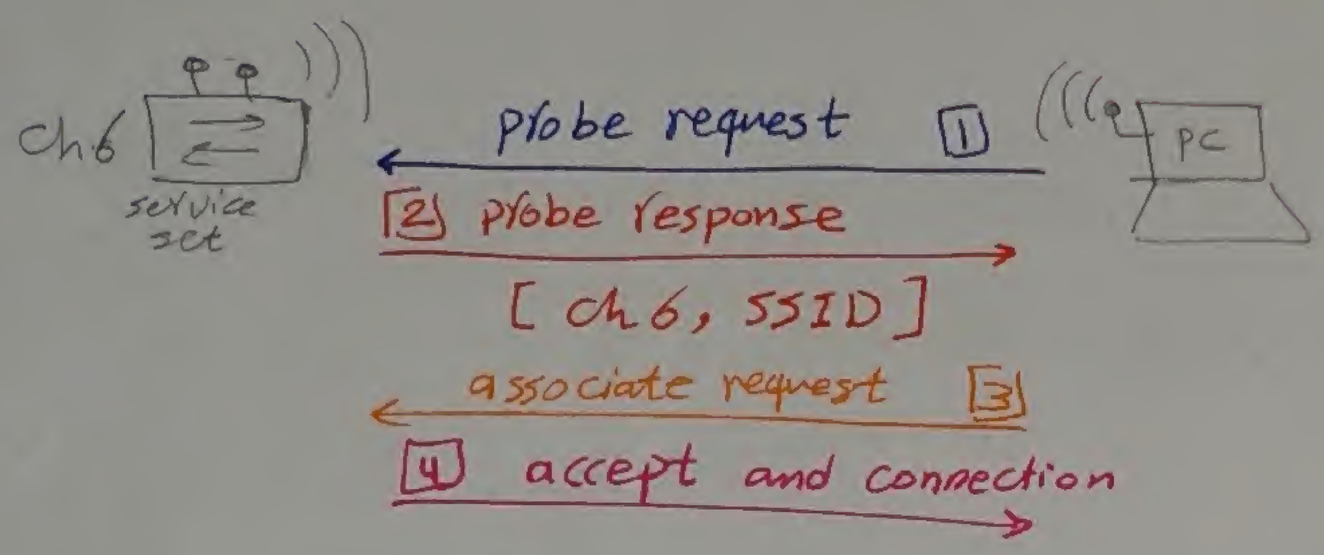
Frequency reuse concept



---

* The operation of service set while communication with pc

SSID : service set ID (access point رقم البطاقه بتاع ال (serviceset)



[1] ال PC بيبعت probe request ودى عباره عن جس نبض على كل ال available channels والعمليه دى اسمها (channel scanning)

[2] ال service set هيرد بـ probe respone وهيبعت فيها اسم ال Channel الخاصه به وال ID بتاعه

[3] ال PC هيبعت associate request وده زى طلب التعامد بالشبكه (regesteration)

[4] Connect & accept

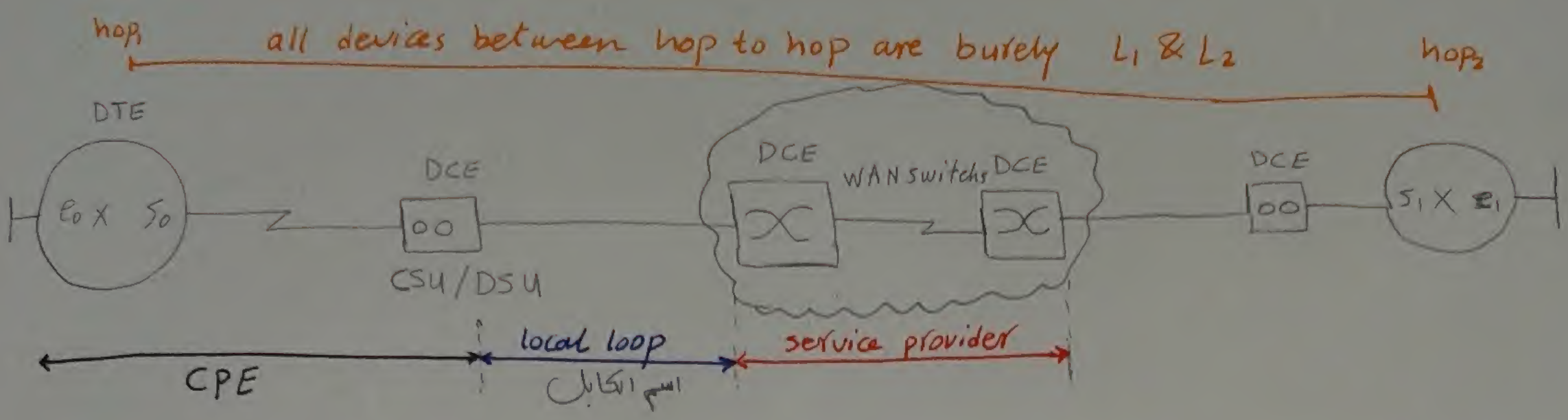
* خطوه / لازم ال PC يكون عارف SSID عشان يقدر ← Network ال associate عشان كده ال access point اللى فالبيت بيبعت ال SSID بتاعه فى ال probe replay و ال access point فى الحاله دى اسمه [public access point]

* ال default على ال access point انها بتعمل Flooding لل SSID بتاعها

* لو ال Ap مش بيذيع ال SSID ← انت لازم تكتب ال SSID بنفسك فى ال PC

الامر على ال PC ← properties ← SSID

WAN switching



* CPE : Costumer premises Equipment [مقر اقامة معدات يتاجه ال Costomer]

* local loop تبع شركه الاتصالات للخلية زى المصرية للاتصالات وبيكونه تحت الارض

CU → <8Mbps
Fiber → >8Mbps

* CSU/DSU : Channalised service unit / Data service unit ⇒ Digital modem

---

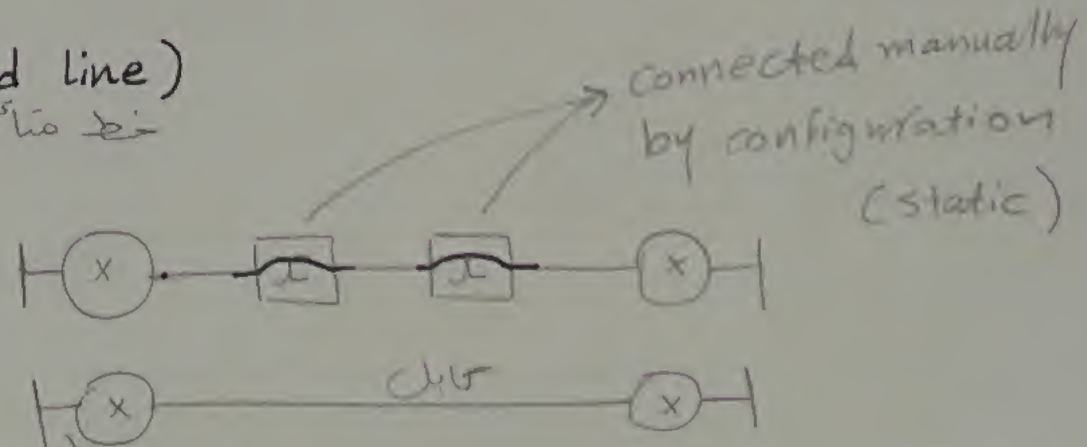
* WAN switching → ① circuit switching
→ ② packet switching

① circuit switching (switching before forwarding)

* physical cable from hop to hop where all data moves on the same path point to point

A Dedicated circuit switching (leased line) خط متأجر

* it is static line
* 24 hr / 7 day gauranteed link
عيبه انه ايجاره غالى اوى طول الوقت



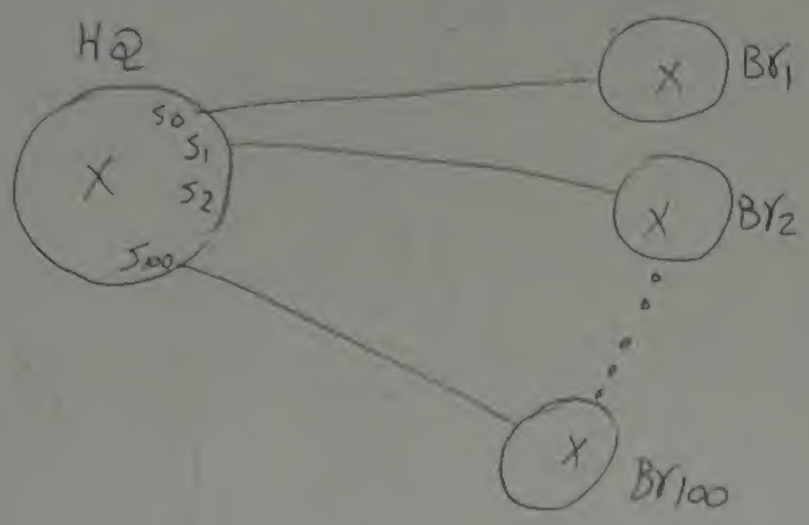
B on demand circuit switching (dial up)

* it is dynamic
- analog dial up قديم → 56 kbps
- digital dial up جديد → 128 kbps : 2Mbps ⇒ ISDN [integrated service Digital network]
غالى جدا

* analog or Digital
⇒ Depend on the Modem type

من العالم دى انت بتأجر الخط لمدة الاتصال فقط
مش طول الوقت زى اوفر

العيب الخطير الـ circuit switching انها بتستخدم point to point only وبالتالى لو انت عندك فروع كتير لشركتك وعايز توصلها للفرع الرئيسى هتحتاج تأجر خطوط كتير بعدد فروع الشركه ← التكلفة هتكون عاليه جدا



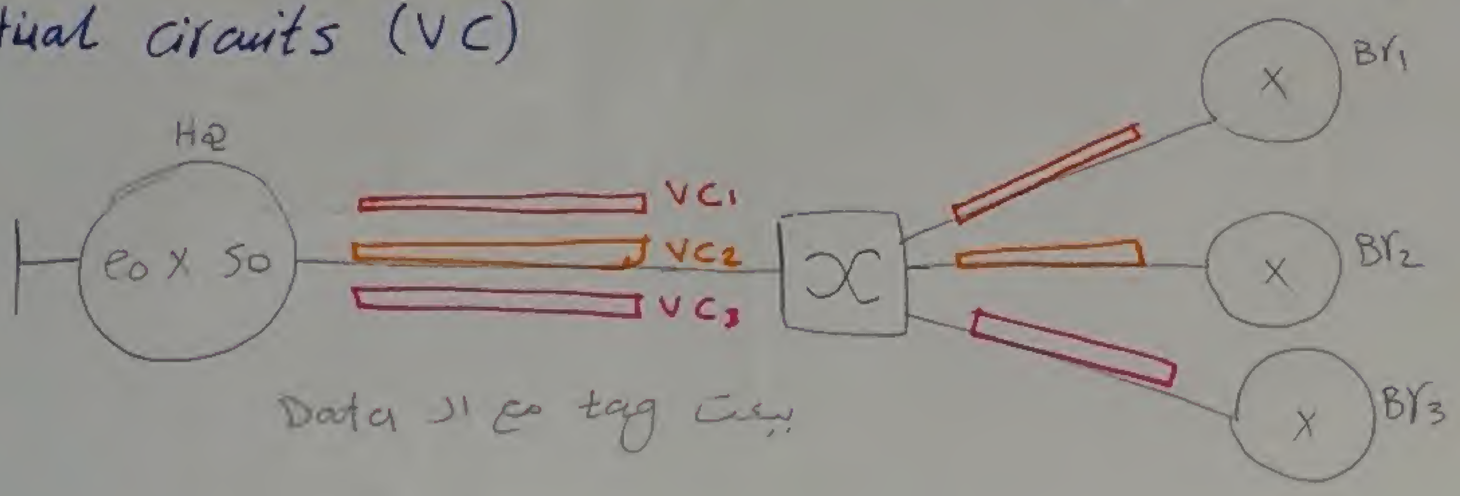
ex. of layer 2 protocols that is used in circuit switching :-

* HDLC
* PPP

---

[2] packet switching (switching while forwarding)

* it is used when point to multipoint switching Topology Based on Vertual circuits (VC)



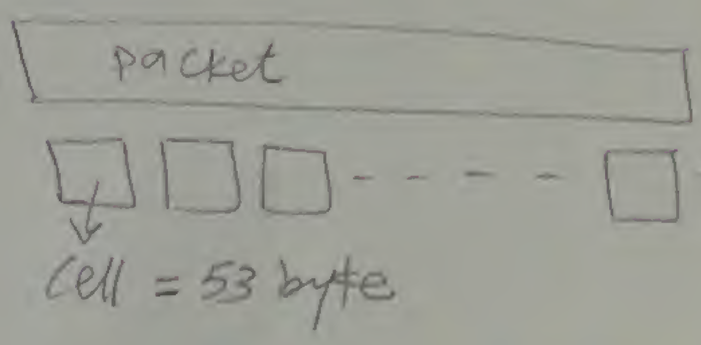
ex: X.25 ⟶ 40 - 45 Kbps ← speed → error correction الموجه بطيئة اوى مشابه بيعمل

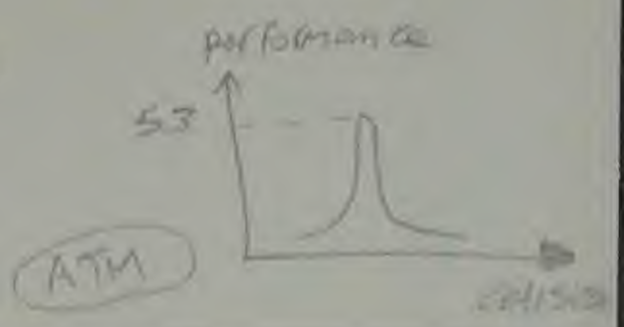
Frame relay ⟶ 40 - 45 Mbps

ATM ⟶ 40 - 45 G bps ← very high cost

(Asyn cronos Transfere Mode)

السرعه الرهيبه فى ATM سببها انه قسم الـ packet الى sub packets اسمها Cell وحجم الـ Cell = 53 byte وبالتالى عمل Enhancement لـ Buffering & processing





Broadband Technology → circuit & packet switching الـ دي غير

it is the use of all Frequencies on the band in order to gain higher speeds

ex: DSL (Digital subscriber line/loop)

* BaseBand Ethernet = 100 m / 1 Gbps
* BroadBand ~ = Modulated Ethernet
= 10 km / 8 Mbps

* DSL is L1 not L3

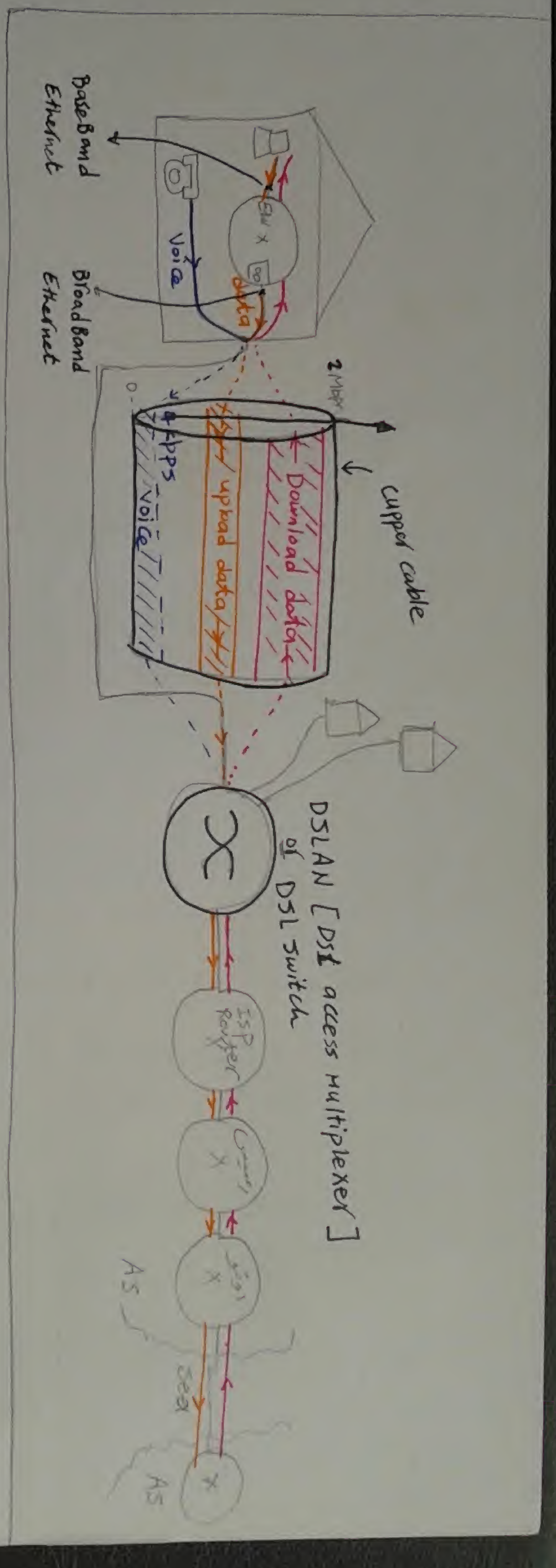
Because it is Modulator demodulator only Between BaseBand Ethernet and BroadBand Ethernet

* DSL has the advantage of CS & PC
جيه كل اثنين

L2 protocols

* L2 : PPPOA (point to point protocol over ATM)
: PPPOE (~ ~ ~ ~ ~ Ethernet)

* L3 : IP/static

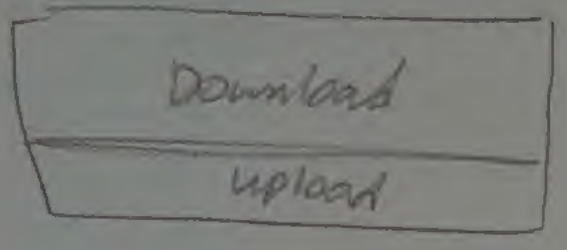


اسم العائلة DSL

ADSL
(Asymetric DSL)

Downbad > upload

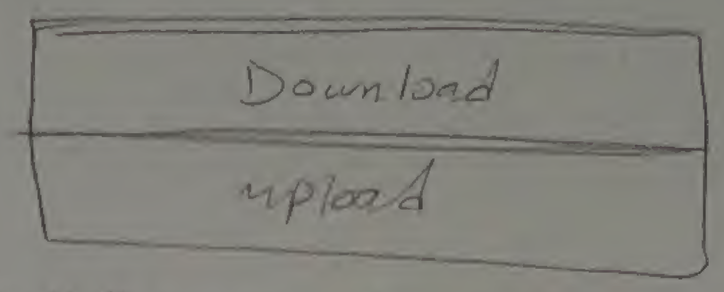
* used for Home users



SDSL
(symetric DSL)

upload = download

* used for Enterprises

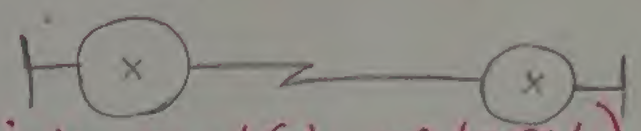


بيل ما الشركه تأجر (leased line) الراوتر

نالس اوى ← بتشترى SDSL

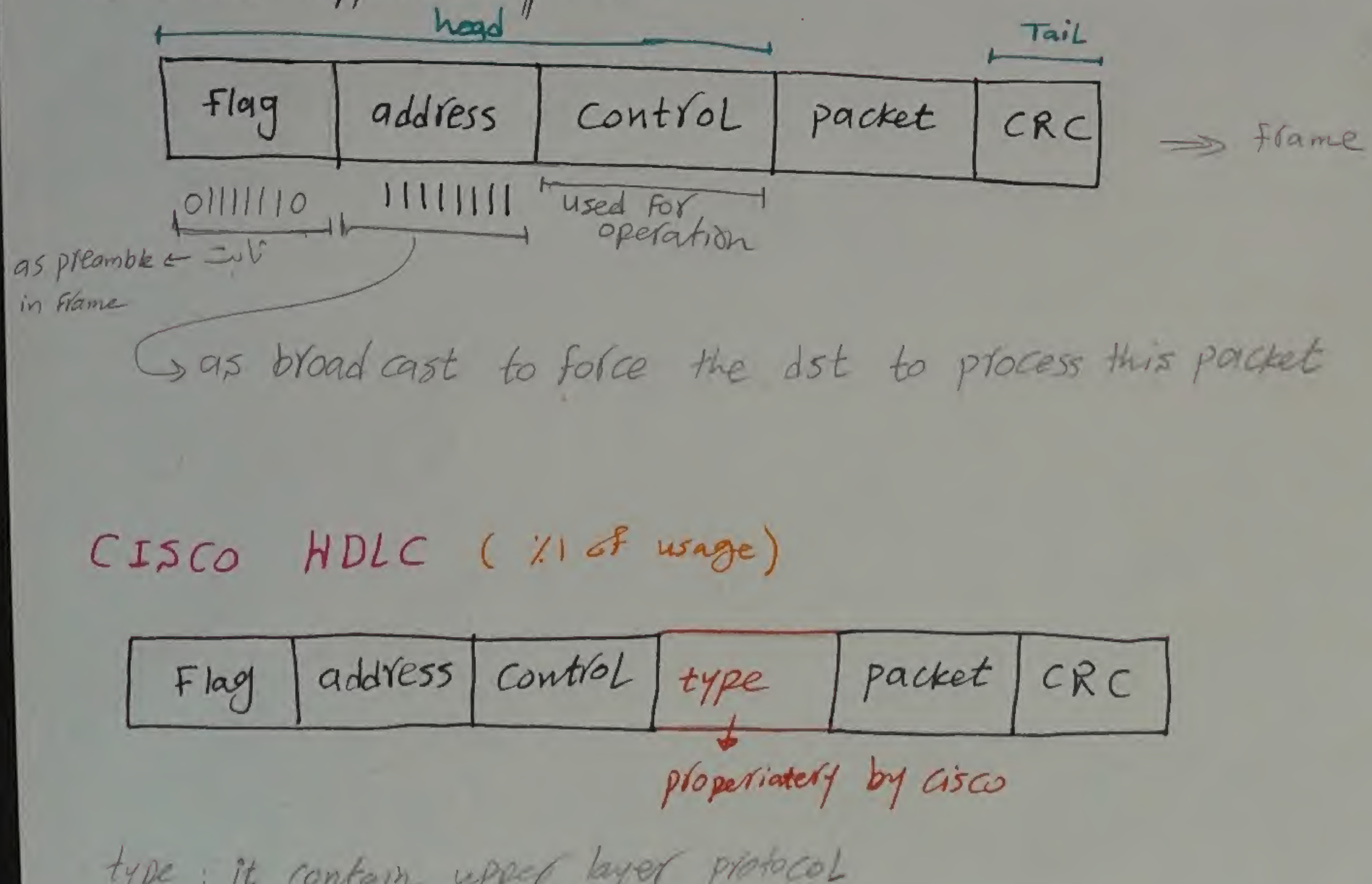
Circuit switching protocols

ⓐ encapsulation



ISO HDLC (High level Data link control protocol)

it is not supported by cisco

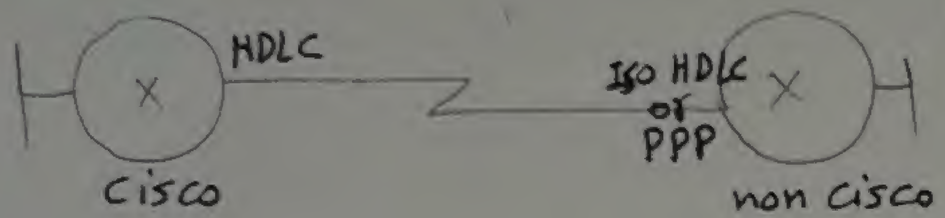


CISCO HDLC (٪1 of usage)

type : it contain upper layer protocol

Note / HDLC is L2 protocol

* the Default of cisco routers in L2 is HDLC protocol and you can change it by configuration

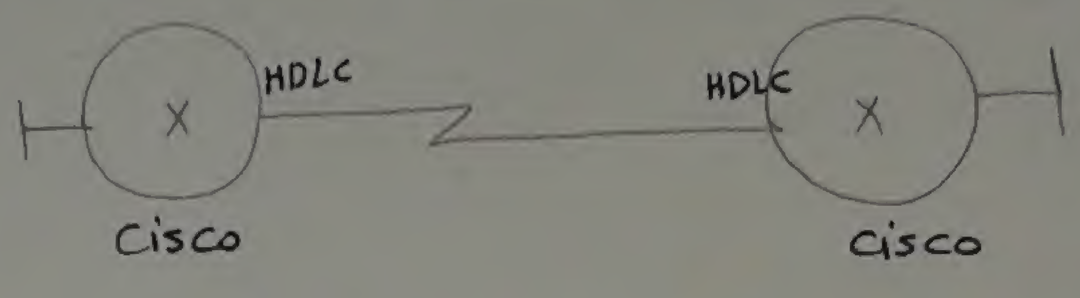


show ip interface breif

status	protocol
L1	L2
up	down

L2 protocol ← الروترين مش قادرين يفهموا

الحل في PPP



show ip interface breif

status	protocol
L1	L2
up	up

* PPP (point to point protocol) ⇒ Standard ⇒ اللي اخترعه الـ IETF وده صيغة تاني عن الـ IEEE

(99% of usage)

L2 protocol

Flag	Address	control	type	packet	CRC

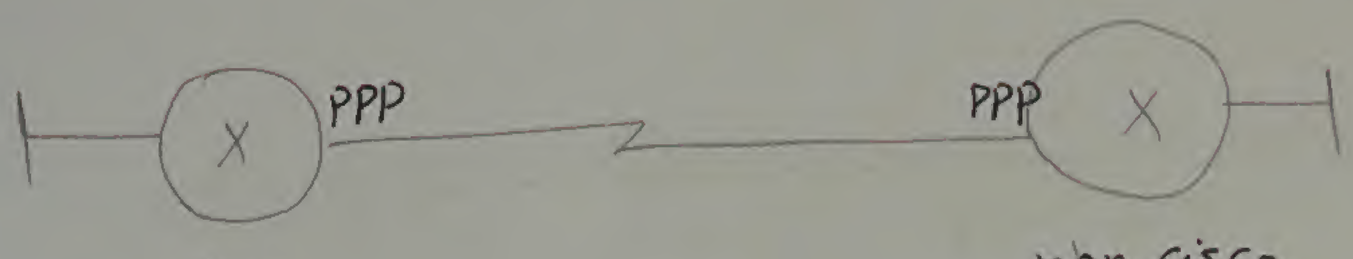
type ↓ Standard

نفس شكل الـ HDLC Frame بتاع cisco بس بأكواد مختلفة

* دلوقتي عشان طريقة الـ configuration تقدر تغير الـ cisco HDLC اللي هو الـ Default اللي الـ routers بقدروا يفهموا L2 protocol وبالتالي PPP

(config)#int s ——

(config-if)# encapsulation { FR | X.25 | PPPOE | PPP } (or between each)



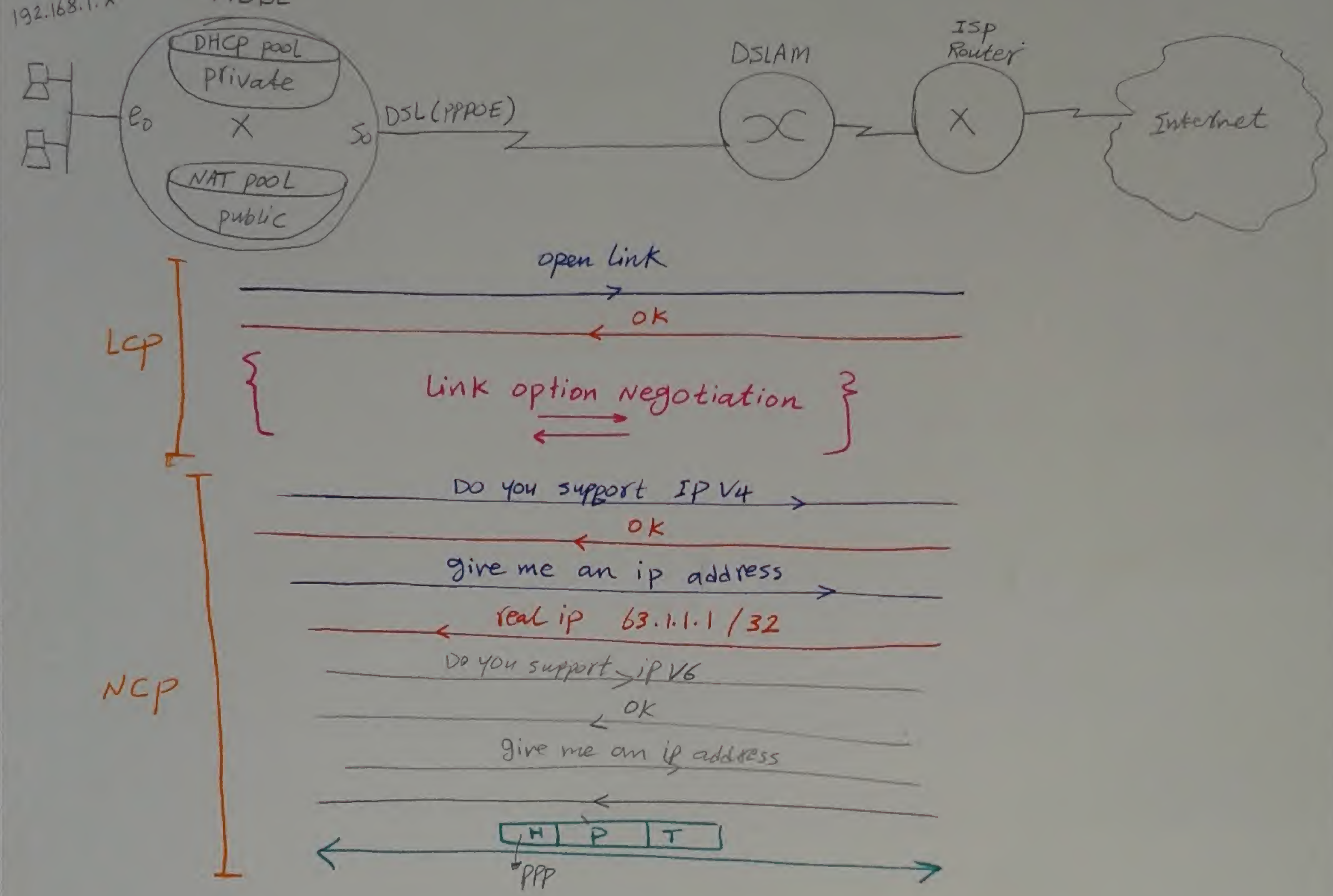
show ip interface breif

status	protocol
L1	L2
up	up

PPP
- leased line
- analog dial up
- ISDN
- DSL
- USB modem (HSDPA)

* PPP operation

to see the operation live press [# debug ppp negotiation]



* LCP (link control protocol)

it is responsiple for
1. establishment link
2. Manage Data link
3. terminate the link

عامل زى الـ TCP بالنسبه للوظائف اللى بينفذها بس الفرق بين دين الـ TCP
TCP for end to end
LCP for hop to hop

* NCP (Network control protocol)

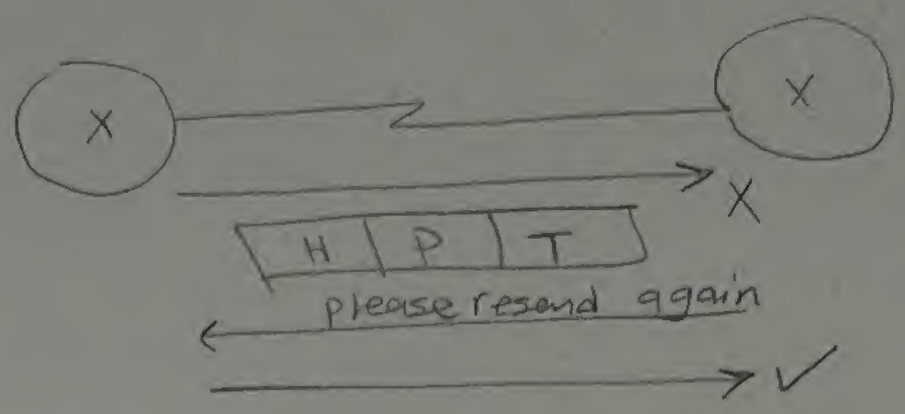
it is responsiple for negotiation the upper layer protocol to be used

* PPP option negotiation

[1] error correction

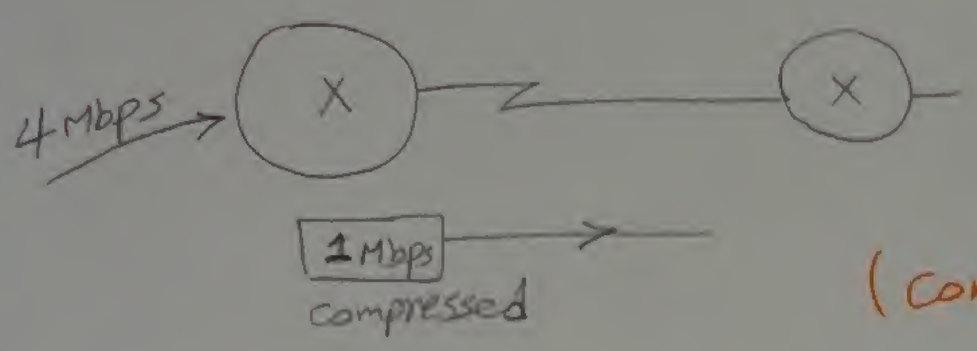
هنا الـ Router يوقع الـ Data صح اللى
بيطلبها قبل ما توصل لـ PC

لاحظ / الروترين لازم يـ support نفس
الـ option عشان يشتغلوا



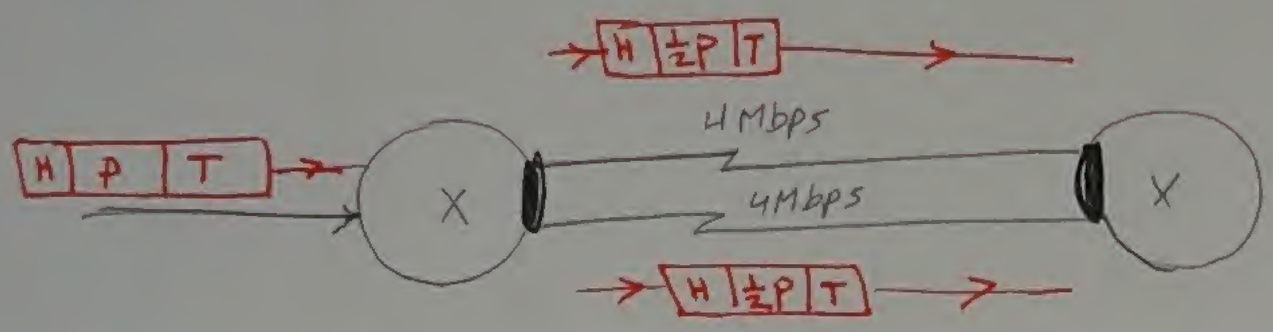
(Config-if) # PPP Collection

[2] Compression



(Config-if) # PPP Compression

[3] Multilink (as load sharing)

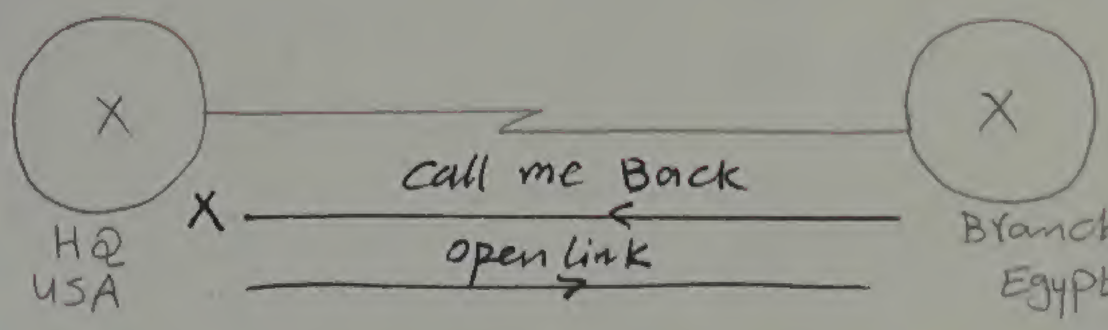


لو انت معايز سرعه 8Mbps والنحاس اقصى سرعه
ليه 4Mbps ← الشركه بتعملك الـ Multilink
وهو زى الـ load sharing بالظبط

⇐ الشركه بتعجزلك خطين (physical) وتعتبرهم اكنهم خط واحد (Verthual)
الـ packet بتيجى عند الروتر الاول هيقطعها نصين ويعطى لكل نص (Head + Tail) ويبعتهم

(Config-if) # PPP Multilink

[4] Call Back



5 cent /min

10 L.E/min

عشان يتحاسب بالتعريفة الاقل

(Config-If) # PPP Call Back

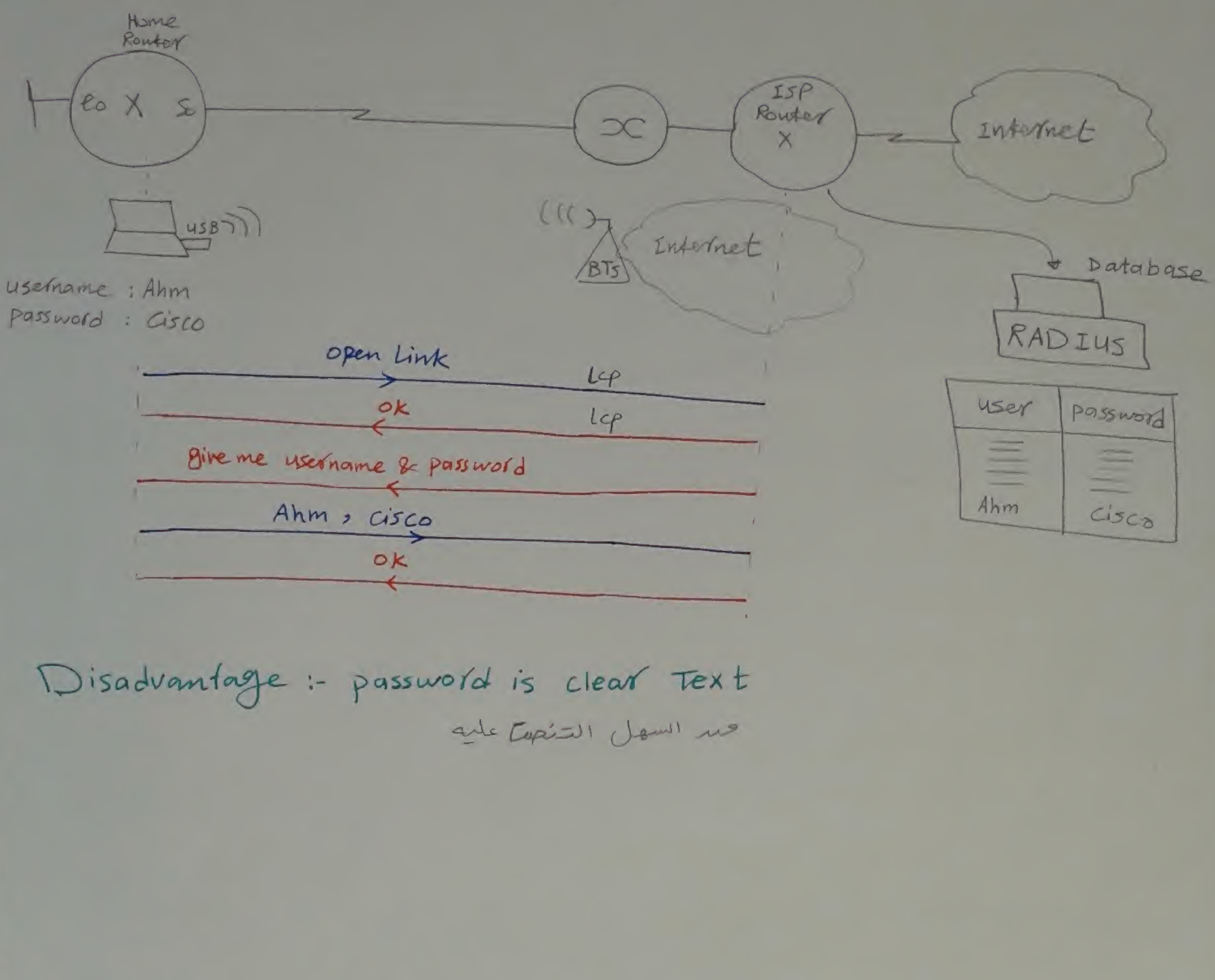
[5] Authentication (username & password)

(config) # int S0

(config-If) # encapsulation PPP

(config-If) # PPP authentication { pap | chap }

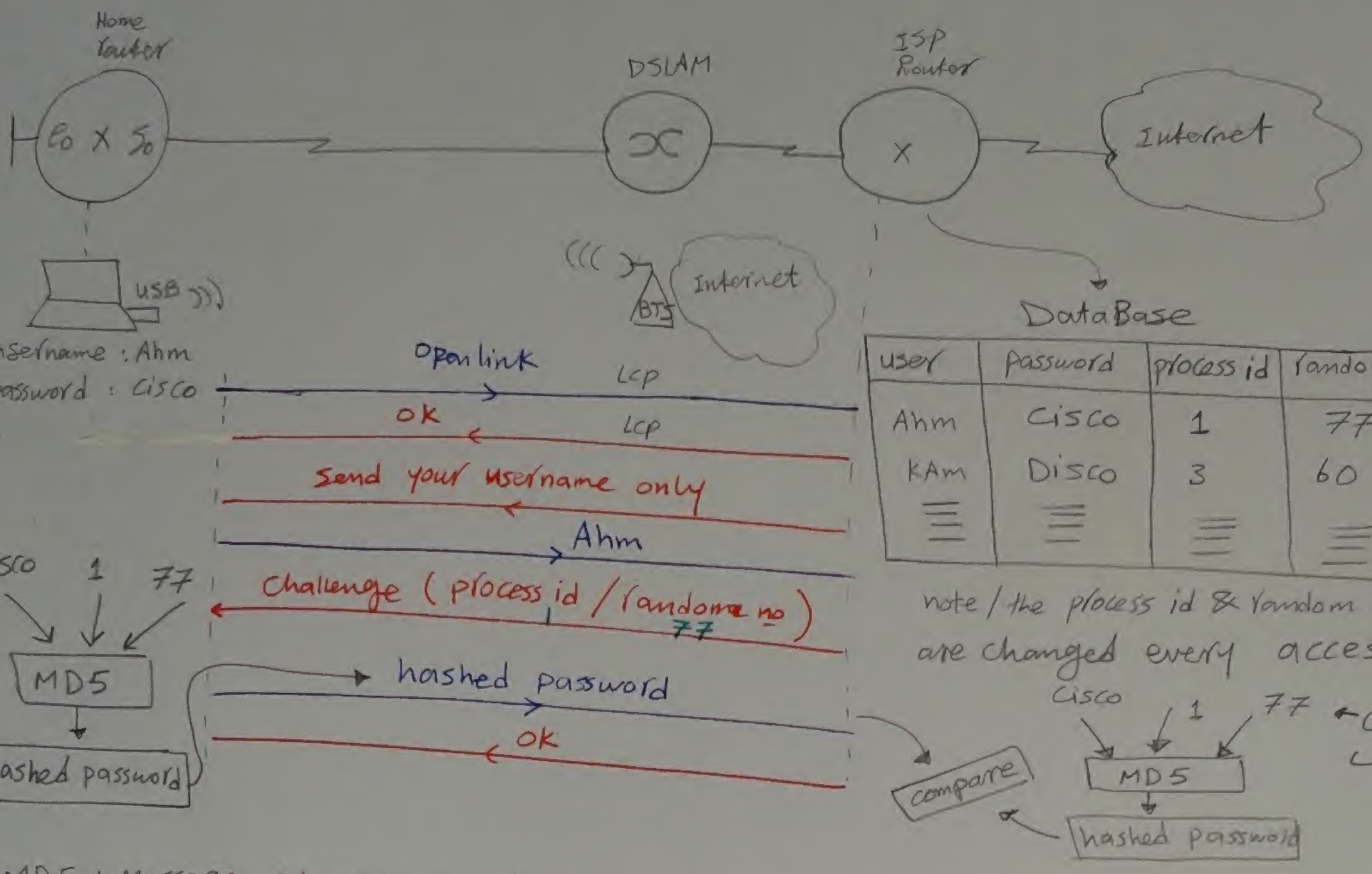
[A] PAP (PPP Authentication protocol)



Disadvantage :- password is clear Text

عيب السهل التنصت عليه

[B] CHAP (Challenge Hand Shake Authentication protocol)



user	password	process id	random no
Ahm	Cisco	1	77
kAm	Disco	3	60
≡	≡	≡	≡

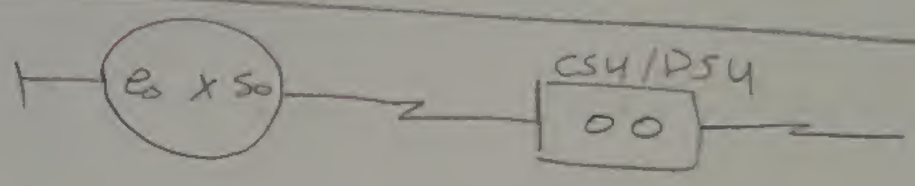
note / the process id & random no are changed every access

MD5 : Message Digester 5 (it is one way function)

pass. الـ تعرف متقدرش ← hashed pass & MD5 يعني لو انت عارف الـ

---

* CSU / DSU [Digital Modem]



* DS0 : Digital service zero (64 Kbps)
* DS1 : Digital service 1

امريكا وكندا T1 — 24 DS0 = 1.54 Mbps

E1 اوروبا — 32 DS0 = 2 Mbps

* DS3

T3 — 45 Mbps

E3 — 34 Mbps

* STM 1 ← بستخدمه مد سنترال اوتو اس اوروبا

155 Mbps

STM2 = 3 4 ...

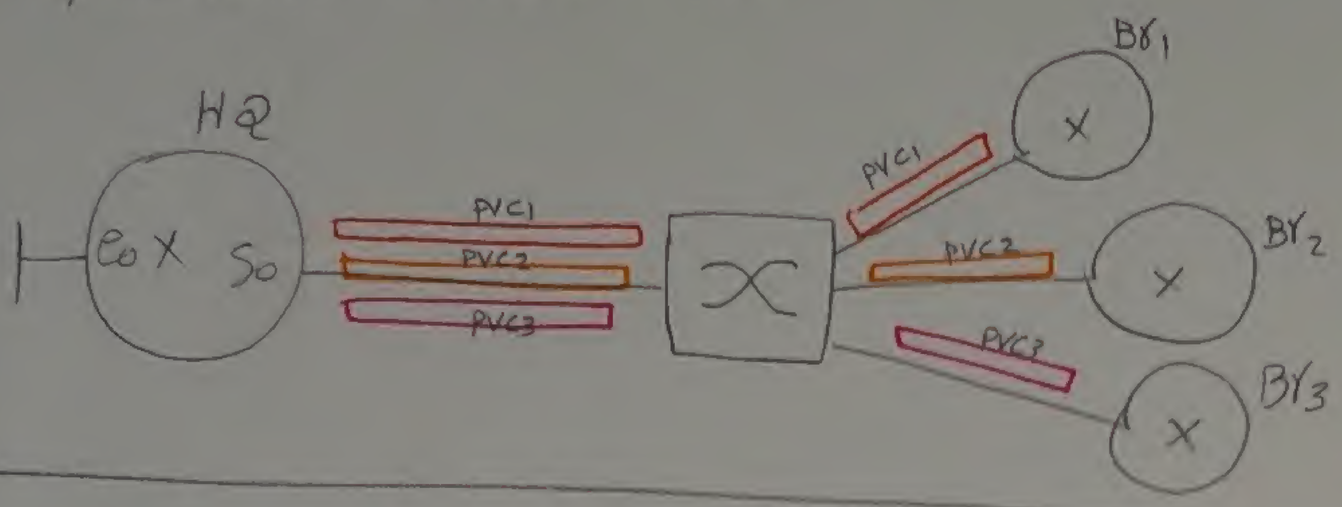
10 Gbps

packet switching

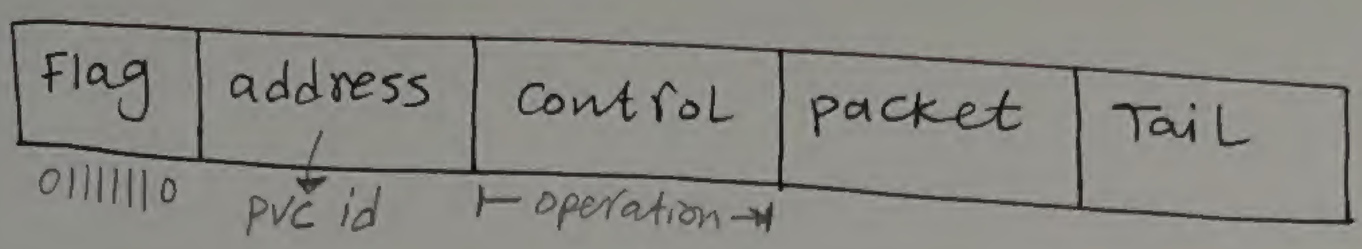
EX: FRAME RELAY → X.25 سرعاته بطيئة جداً وال ATM الاكثر استخداماً لأنه ال غالي اوي

it is point to multipoint packet switching based on PVCs

PVC : permenant vertual circuit

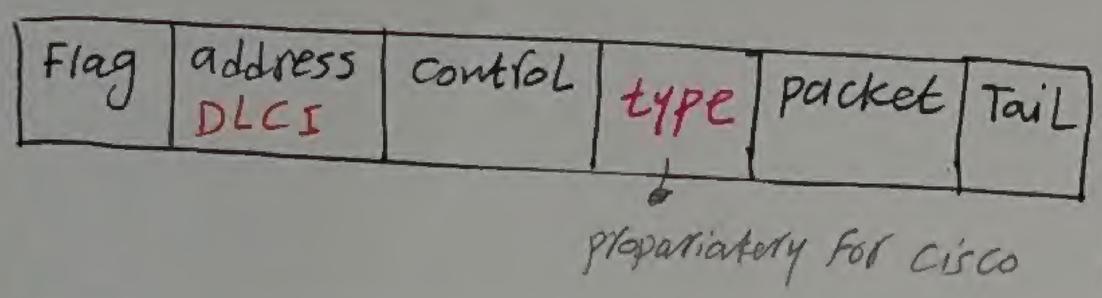


FR encapsulation * is called LAPF (link access procedure for FR)
protocol

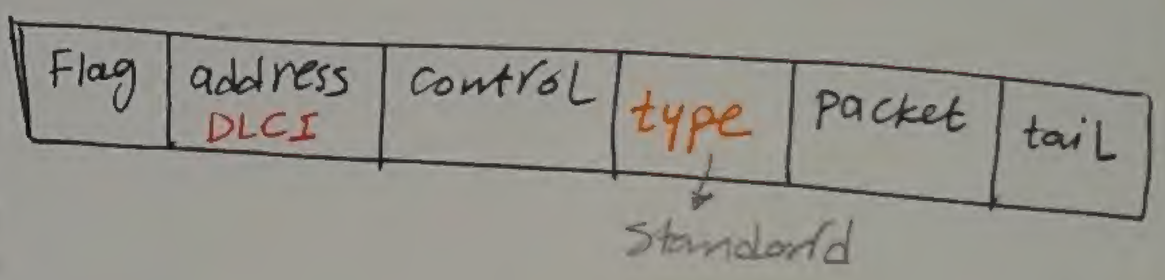


نوع من ISO HDLC

Cisco LAPf



IETf LAPf



*address

X.25 → X.25 no → PVC id (8 bit) ↔ 0 … 255

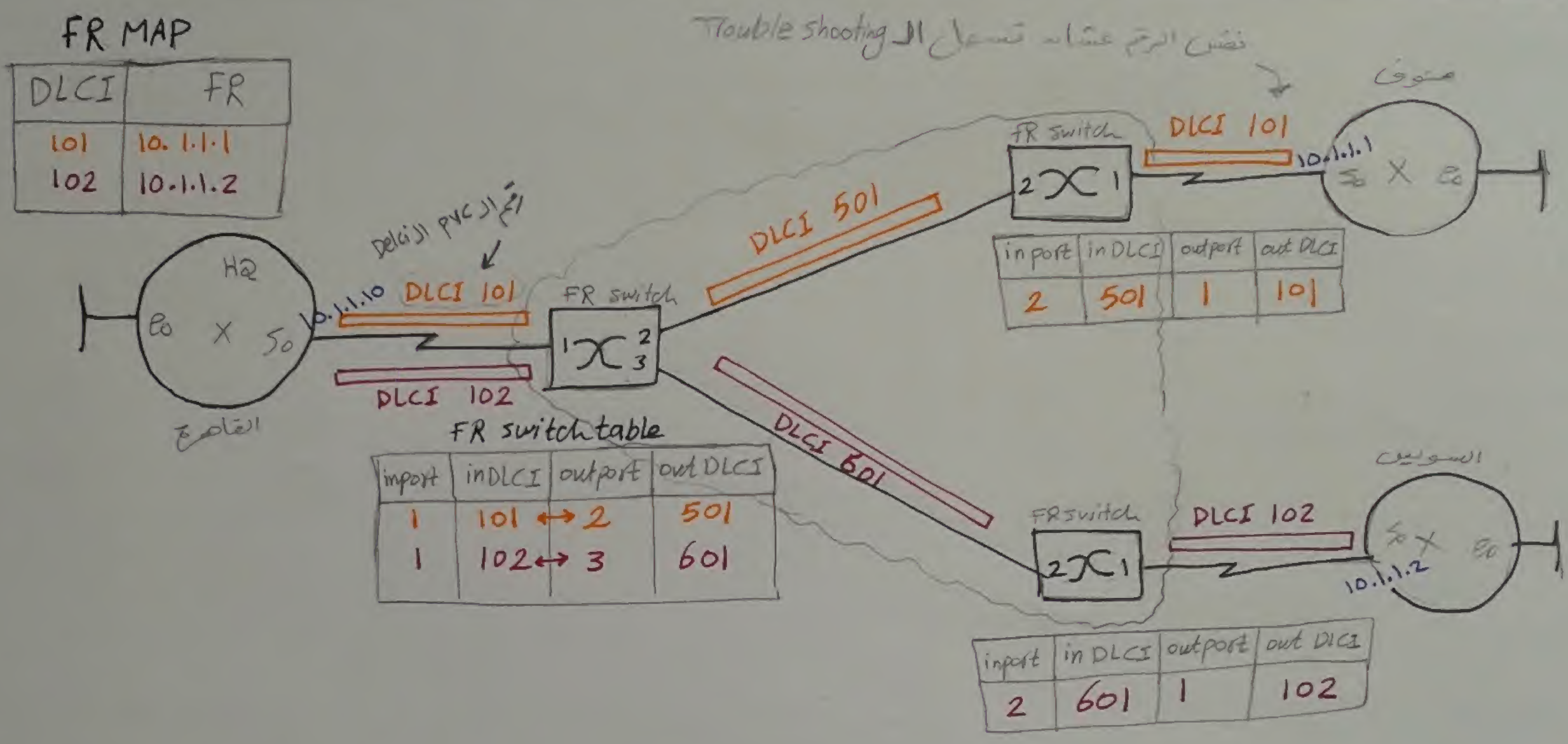
بعض انك ممكن تعرّف على 256 PVC على نفس ال Physical cable

FR → DLCI (Data link circuit identifier) → PVC id (10 bit) ↔ 0 … 1023

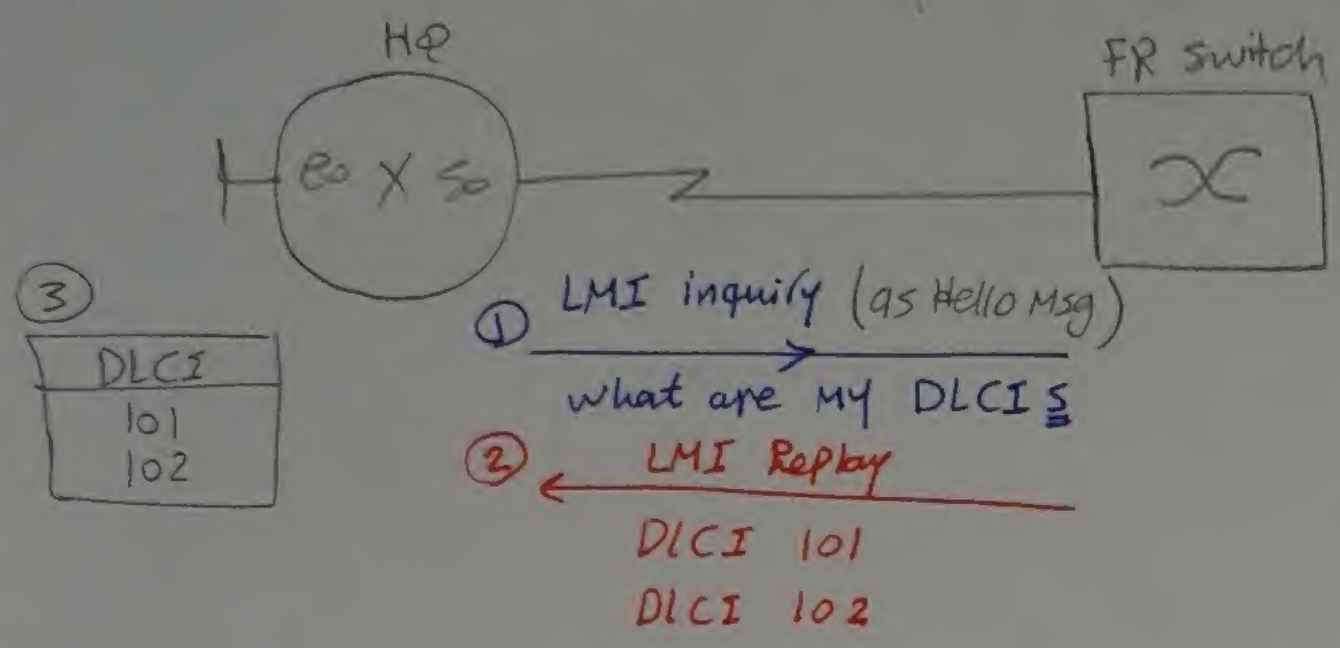
ATM → VPI/VCI (vertual path id / vertual circuit id) → PVC id (16 bit) ↔ 0 … 65535

FR operation steps:-

1- FR switch statically configures its PVCs using LMI
2- FR router dynamically discovers its DLCI to next hop router using IARP
3- FR router dynamically map DLCI



* The second step is LMI operation
  * LMI (local Management interface)
  * it is as hello msg to be sure that the PVCs are keepalives



[active يعني ال PVC شغاله من الاطرفين والسكه كلها سليمة]

[inactive يعني ال PVC سليمة جنبي لكنه من فصل او قطع بعيد عني] ← DLCI بيكتب جنب

[Deleted يعني ال PVC اللي جنبي مباشرة failed او الconnection فاصلة]

* Types of LMI

1- cisco LMI

2- q933a LMI ⇒ Made by ITU (international Telecomm. Union)

3- ANSI LMI ⇒ ANSI (American National Standard I--)

4- dynamic (auto) LMI discovery ⇒ Made by cisco & it is the default for cisco devices

وهنا الروتر هيبعت LMI inquiry بالطريقة الاولى لمدة 6 مرات (دقيقة) ما لو الـ switch مردش ← الروتر ~ ~ ~ ~ ~ ~ الثانية ~ ~ ~ ~ ~ ~

The configuration

```
(config)# int S0
(config-if)# incapsulation Frame-relay [ietf]
(config.if)# Frame-relay LMI-type {cisco | ANSI | q933a}
X(config-if)# Frame-relay MAP ip 10.1.1.1 dlci 101
X(config-if)# Frame-relay MAP ip 10.1.1.2 dlci 102
```

inc FR ← اختصار

option ↙

cisco لو هتكتب حاجة تانية غير by default ←

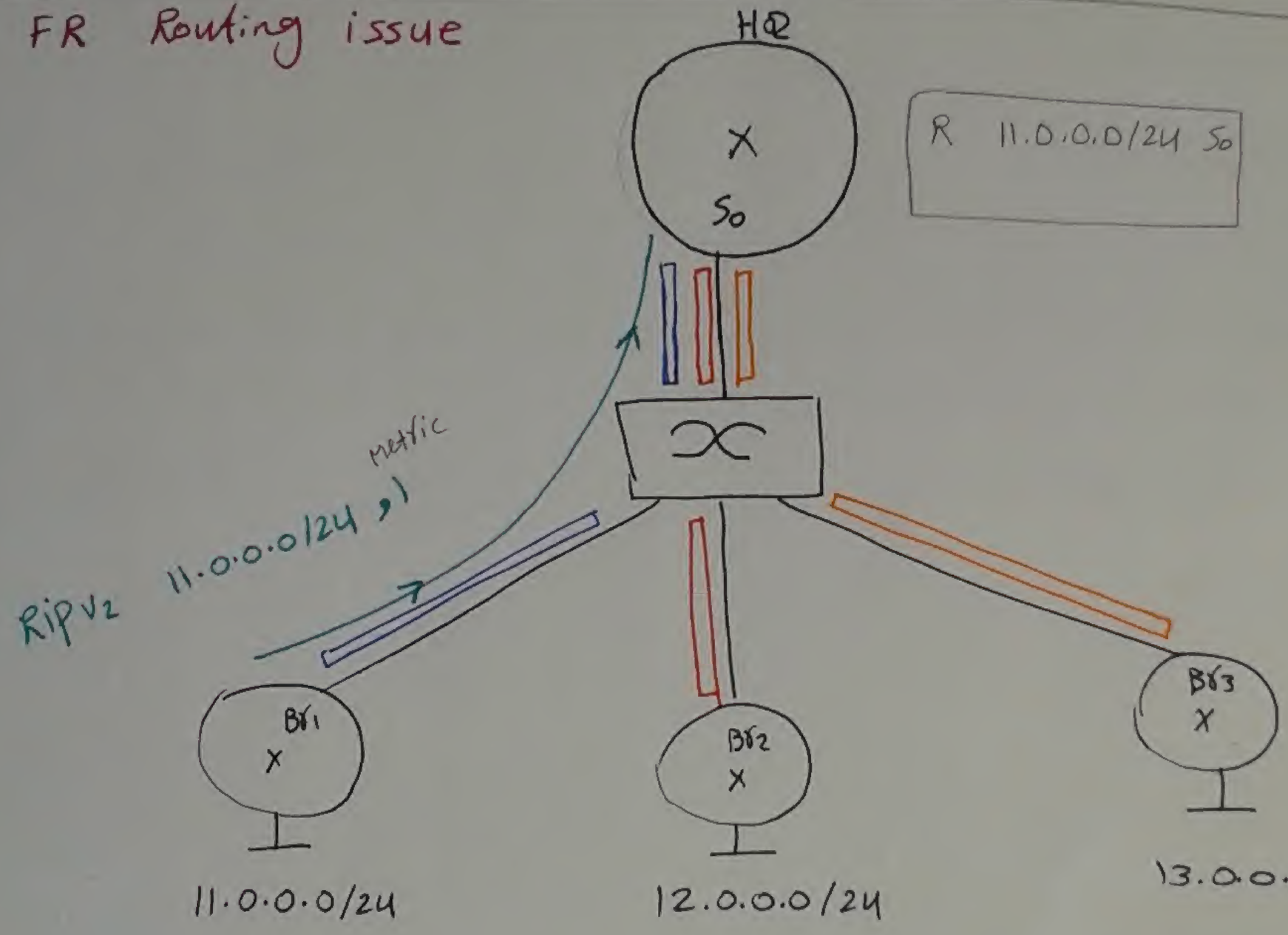
Statically

لو لم تكتب الامرين دول ع الروتر هيشتغل IARP ← Dynamically

لو لم تكتب الامر ده ع Router cisco هيختار ← dynamic LMI discovery

---

FR Routing issue



المشكلة هنا ان لو Br1 بعت الـ RTG Table بتاعه لـ HQ ع الـ HQ هش هيعرف يبعت الـ RTG Table بتاع Br1 لـ Br2 & Br3 عشان خاصية الـ Split Horizon اللي بتقول لو اتعلمت حاجة من Interface معين ع هينفعش تخرج نفس الحاجة على نفس الـ Interface

وكده اتحل ف .....

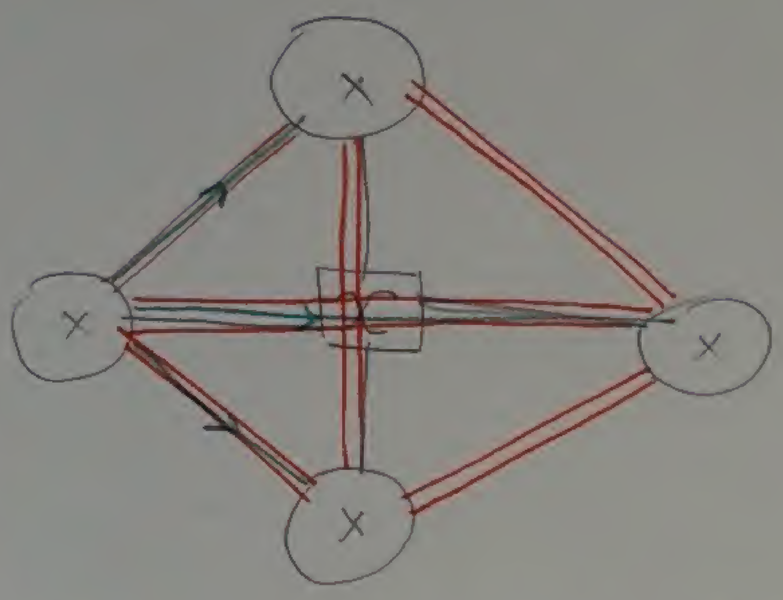
Solutions :-

[1] disable split horizon

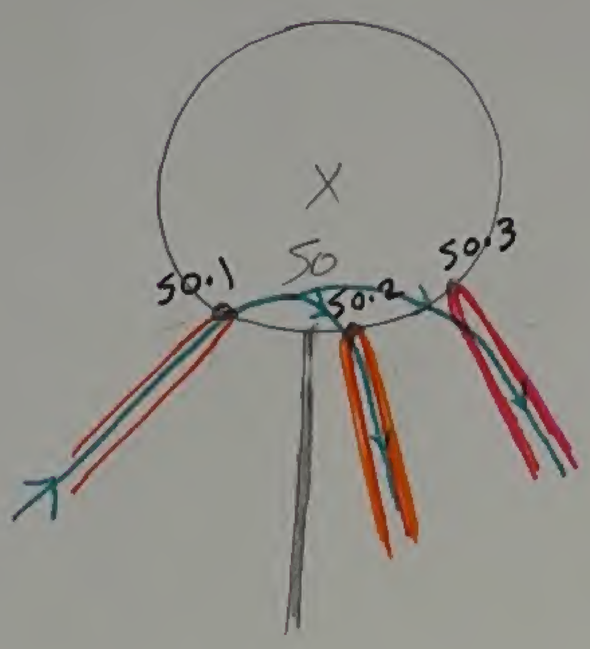
(config-if) # no ip split horizon ⟹ الشكله انك صنعت فى مشكلة الLoops

[2] use Static (مش هينفع لو الشبكه كبيره اوى)

[3] use full Mesh topology ⟹ حرام عليك التكلفه والتعب



[4] Devide Main interface into point to point subinterfaces (99% of usage)



(config) # int S 0.1

(—subif) # ip add —— ——

Security

Security attacks

(1) Reconaissance attack (استطلاع)

trying to discover network resources

- no of PCs
- no of switches
- no of routers
- servers
- services (Application)
- IP range
- MACs

(2) Spoofing attack ≡ MASK querating (تقمص)

- IP spoofing
- MAC spoofing
- Router spoofing

Spoofing ≡ sniffering ≡ earsdropping (تجسس / تصنت)

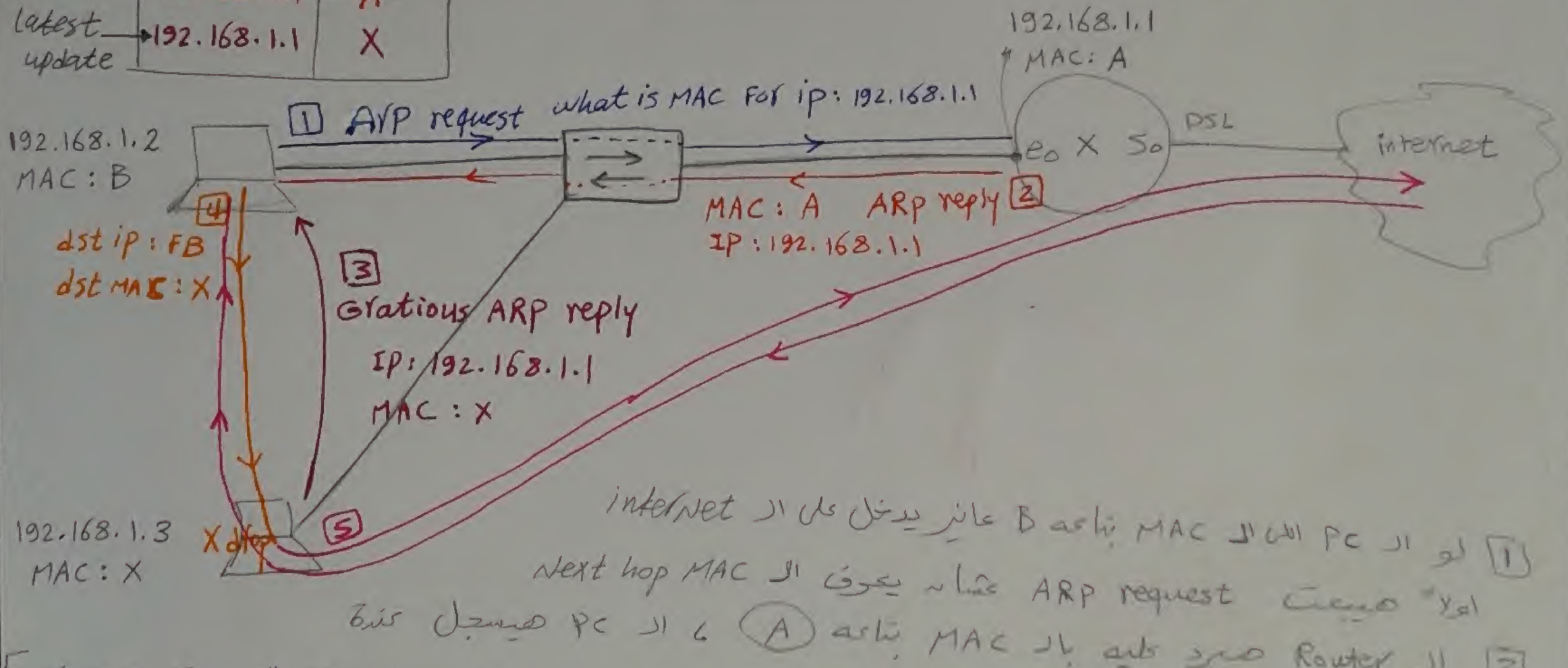
(تلصيص)

ARP cashe

IP	MAC
~~192.168.1.1~~	~~A~~
192.168.1.1	X

latest update

Router spoofing



1 لو الـ PC اللى الـ MAC بتاعه B عايز يدخل على الـ internet عشان يعرف الـ Next hop MAC اللى هو الـ Router صيبت ARP request "او/و" صيبت على الـ PC يسجل كدة ، الـ Router (A) بتاعه MAC

2 الـ Hacker صيد عليه بالـ MAC & IP ← الـ ARP cache [ملحوظة: تقدر تشوفها فى الـ DOS بالامر arp -a]

3 الـ Hacker صيبت Gratious Arp عشان يوهم الـ PC انه هو الـ Router وبيقوله فيه الـ Router IP والـ Router MAC = X

4 ولوقتى الـ PC بيحذف الـ latest update اللى فيه الـ MAC = X وبيضع الـ ARP cache الاخير من الـ

4 لو الـ PC عايز يدخل على الـ FB مثلاً ← بيبعت طبقاً للجدول اللى عندة لازم يبعت الـ Default gateway اللى الـ MAC بتاعه X وبالتالى لما الـ Data تتروح على الـ Hacker ، الـ Hacker هيوقعها (drop)

(5) ممكن ال Hacker يكون اشرس ويتصنت على الداتا فبالتالي يبعتها على ال Router ولما الروتر يرد عليه هيبعت الرد على ال PC ، والحاله دى اسمها

(MAN in the Middle)

* حشان تعرف هل بيتم التصنت عليك ولا لأ ← اعمل Tracert على ال Dos وهو هيجيب لك ال Next hop IP ، لو ال Next hop IP هو ال Router بتاعك يبقى تمام ، لو حد بيتصنت عليك هيجيبلك ال IP بتاع ال hacker مش الروتر

* حشان تمنع حد انه يغيرك ال MAC بتاع ال Gateway ممكن (Router) عن طريقه الاحرف تكتب ال MAC و ال IP بتاع ال Gateway بايدك Static

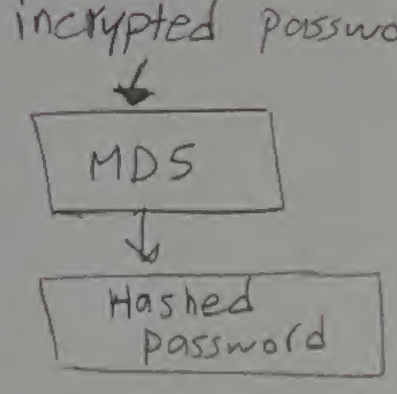
arp -s IP MAC

لازم عيبه انك لو عملت Restart لل PC هتضطر تكتبه تاني

(3) Brut force attack
password guessing

* هنا بيجرب passwords كتير اوى وبيدخلها عند MD5 algorithm

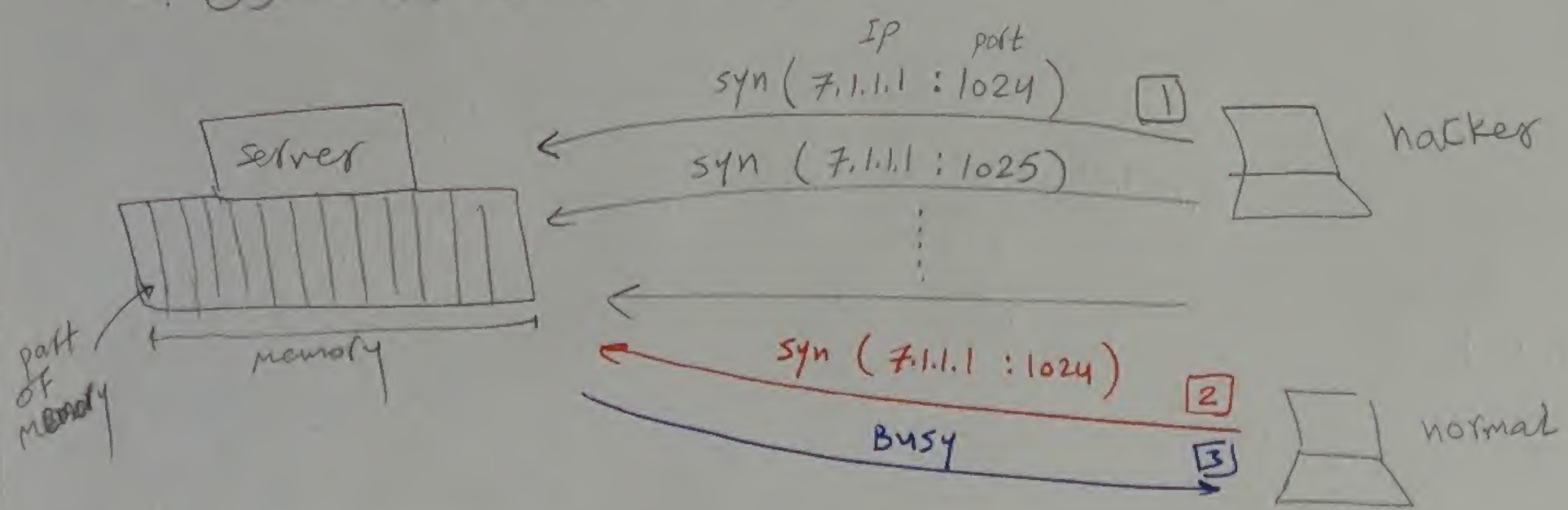
لحد ما تطابق الـ Hashed pass. وبكده بيقدر يطلع الـ password



Try ⇒ If error
Try new one and so on

(4) DOS attack [Denial of service]

هنا عايز يوهم ال Server انه ناس كتير بتدخل عليه وانه مشغول طول الوقت ولو حد عايز يدخل على ال Server ⇐ ال Server هيمنعه يدخل لأنه مشغول جداً



الطبيعى لما pc بيبعت فتح session جديدة مع ال server ، ال server هيجزله جزء من ال memory

1 ال hacker هيبعت فتح sessions كتير جدا" فى الثانيه الواحدة ، وكل session جديدة بتتفتح ، ال server بيحجزلها جزء memory ، هنا ال hacker هنا اله يشغل ال memory كلها بتاعه ال server وبالتالى لو جه pc 2 عادى وعايز يفتح session جديدة مع ال server ← 3 ال server صيد عليه اله مشغول جدا" و مش هيفتح معاه اى session

⇐ الحل هنا اله ال server ميقبلش يفتح اكتر من 5 sessions مثلا" لنفس ال pc فى الثانية

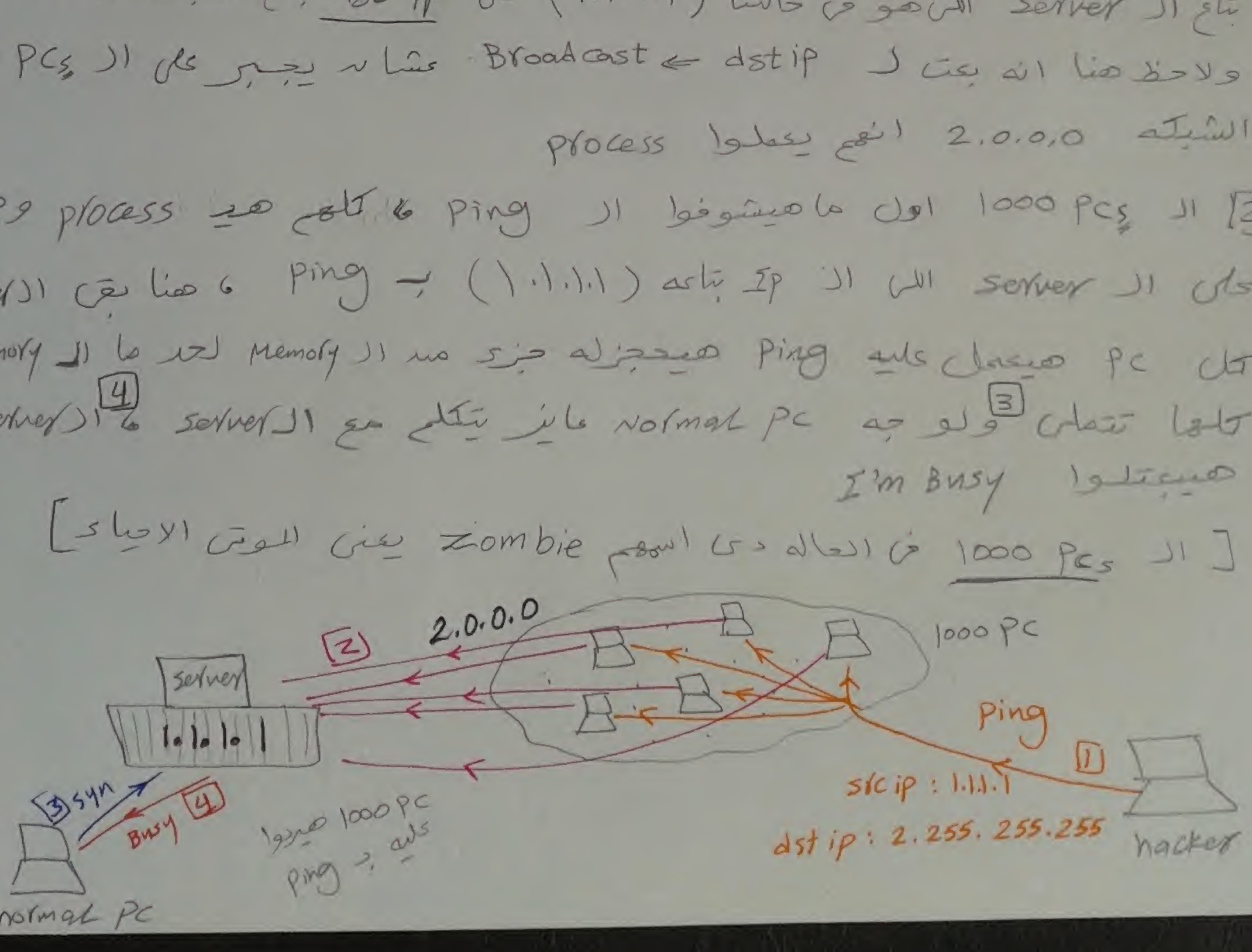
⇐ هل ال hackers هيسكتوا ؟؟؟ لأ طبعا" . دة اكل عيش !! حشاله كمدة هيفكروا فى الحل دة ⟸

DDOS attack (Distributed DOS)

1 ال hacker هيروح على شبكه مثلا" فيها 1000 pcs وهيبعت لهم src ip → Ping بتاع الشبكه 2.255.255.255 على dst ip بتاع ال server اللى هو فى حالتنا (1.1.1.1) ولاحظ هنا انه بعت لـ dstip ← BroaCast حشانه يجبر كل ال pcs فى الشبكه 2.0.0.0 انهم يعملوا process

2 ال 1000 pcs اول ما هيشوفوا ال Ping كلهم هيه process وهيروحوا على ال server اللى ال Ip بتاعه (1.1.1.1) بـ Ping ، هنا بقى ال server و كل pc هيعمل عليه Ping هيحجزله جزء من ال Memory لحد ما ال Memory كلها تتملى 3 ولو جه normal pc عايز يتكلم مع ال server ، ال server 4 هيبعتلوا I'm Busy

[ال 1000 pcs فى الحاله دى اسمهم Zombie يعنى الموتى الاحياء]



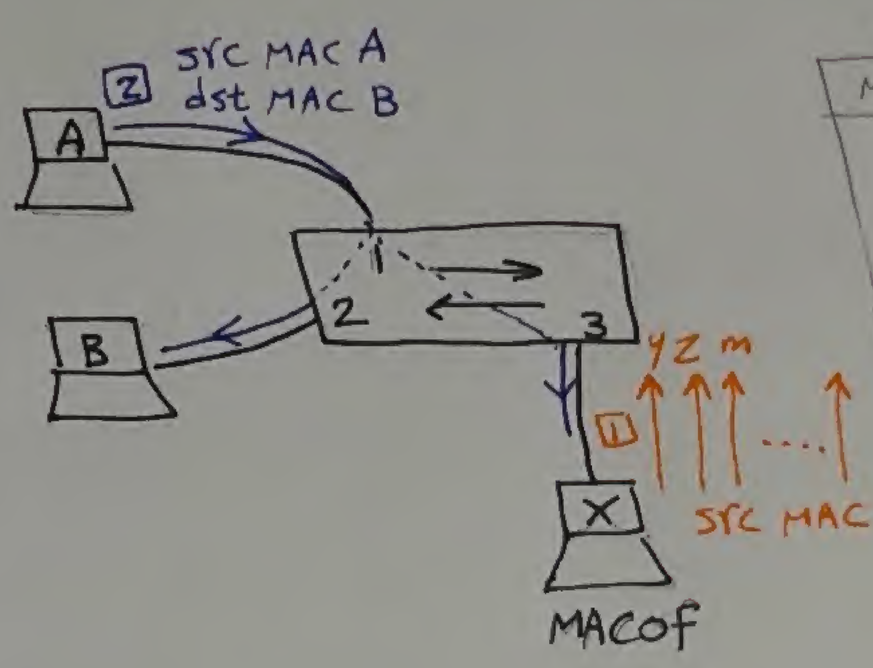
Security Mitigation مداواه الالام والجراح

1) Switch security

تأصيل المشكلة

1 من واحد اسمه MACOF عمل برنامج على اسمه ، اول ما الـ switch هيفتح ، البرنامج ده هيبعت [SRCMAC ، SRCMAC Z ، SRCMAC Y .....] يعني هيعلم الـ switch ماكات كتير جداً [وهما مش موجودين اصلاً] ، كل اللي هيعمله الـ switch انه كل ما هتجيله MAC جديده هيروح حفظه من الـ MAC table بتاعه لحد ما الـ MAC table يتملى

2 لو جه PC حقيقي عايز يبعت حاجه لـ PC تاني ، اولاً لازم يعدّي على الـ switch ، الـ switch هياخد الـ dst MAC وهيقارنه بالجدول اللي عنده ، مش هيلاقيه موجود في الجدول فيهيضطر انه يـ Flood ، هيجيب الـ Hacker هياخد الـ Data اللي جايه من الـ Flooding وهيتصنت عليها [هنا الـ swich بقى عامل زي الـ Hub]



MAC table

MAC	Port
Y	3
Z	3
M	3
...	...

switch port security

(config) # interface FastEthernet 0/3

(config-if) # switchport port-security

- ① only one MAC allowed to access (عايز)
- in case of Violation ⇒ port will shutdown by default (لو حصل في وش الكل)

option

(config-if) # swith port port-security Maximum 5 ← لو عايز تحدد اكبر عدد مسموح اللي مسموح لها تدخل على الـ port دي ولو 6 مثلاً دخلوا على الـ port ⇐ الـ port هتقفل bydefault ⇐ shutdown

(config if) # switch port port-security MAC MACA
(- -) # ~ ~ ~ ~ MAC MACB ← لو عايز تسمح لـ PC محددة تدخل على الـ port دي ولو PC له MACY مثلاً دخل على الـ port

ممكن متكتبش الاخرين دول وتكتب الاخيرة

(config if) # switch port port security sticky

(config-if)#switchport port security violation {restrict | protect}

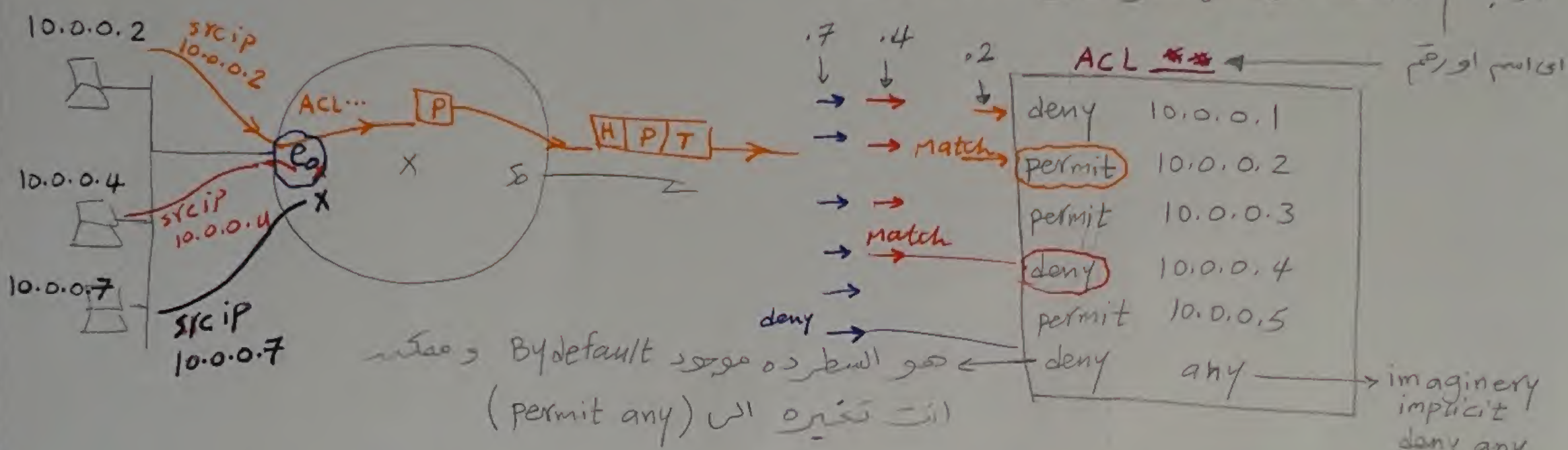
الامر دة بتكتبه لو فى حاله التعدّى او الاختراق مش عايز الـ port تقفل (shutdown)

permit → normal فى وش كل الناس ، تكمل عايز تفلتر الناس بمعنى
deny → hacker

⇐ لو لم تكتب الامر دة هيبقى الـ default هو (لو فى حاله اى تعدى) ⇐
Shutdown

Router security

ACL [Access control list] → اى اسم او رقم ← security ← الى معروفش معدّهوش



هو السطر ده موجود By default وممكن انت تغيره الى (permit any)

الترتيب مهم اوى وانت بتكتب الـ ACL عشان بيمشى سطر سطر ولو لقى الـ IP اللى داخل مطابقه لسطر معين مكتوب بالفعل فى الـ ACL ← هينفذ اما access او Deny على حسب المكتوب فى السطر اللى فيه الـ IP ، ولو ملقاش الـ Ip فى الـ ACL هينفذ الـ Default اللى هو (deny any) الا فى حاله انك كاتب اخر سطر (permit any)

* ملحوظه قبل ما تكتب الـ ACL لازم تعرف الاول على اىّ Interface (فى حالتنا Eo)

ACL Types

- Ip standard ACL
  - old → numbers (1 - 99) (1300 - 1999)
  - new → name (any name)
- Ip Extended ACL
  - old → numbers (100 - 199) (2000 - 2699)
  - new → name (any name)

① Ip Standard ACL

it filters data based on src ip only

A create ACL

numbered :

لازم تكتب واحد مابين الاقواس { }

(config) # access list 1-99 { permit | deny } src ip [wild card mask]

option

① الـ wild card MASK دي option وهو بياخد من 32bit ⇐ (0000...1111)

لو الـ bit = 0 يعني عايز الـ bit القابله له في الـ IP بالتحديد

لو الـ bit=1 يعني X (don't care)

لو مكتبتش الـ wild card MASK في الـ Command هيبقى الـ Default اللي هو 0.0.0.0

يعني انا عايز الـ IP دة بالتحديد

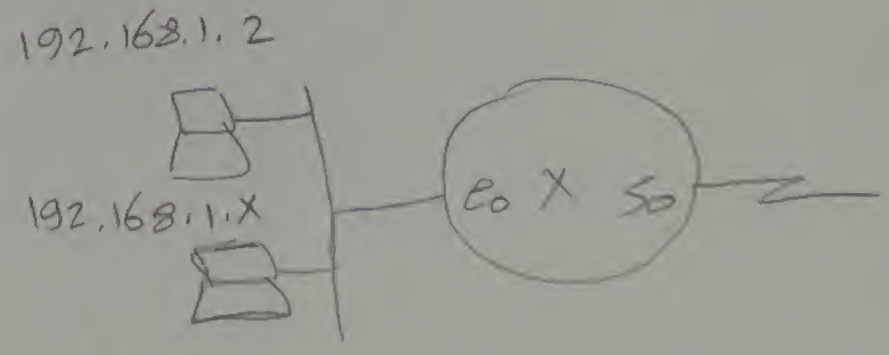
EX1 (config) # access list 7 permit 192.168.1.10

معناه ان عايز الـ IP دة (192.168.1.10) بالتحديد يبقى permit

EX2 (config) # access list 7 deny 192.168.1.0 0.0.0.255

معناه ان عايز الـ IPs دول (192.168.1.X) اللي هما (192.168.1.0 ↔ 255) كلهم deny

ملحوظة / ترتيب السطور مهم جداً في الـ access list فمثلاً



(config) # access list 7 deny 192.168.1.2

(config) # accesslist 7 permit 192.168.1.0 0.0.0.255

* بالامرين دول هو لو جاله (192.168.1.2) هيشوف السطر الاول و هيمنعه من الـ access

* تكمن لو غيرت ترتيب السطرين ، في الحاله دي اول ما هيجيله (192.168.1.2) هيشوف السطر الاول (192.168.1.X) فيعديه و بكده السطر التاني مش هيكون ليه اي لازمه

named :-

(config) # ip access-list standard name

(config-std-nacl) # {permit | deny} src ip [wild card mask]

standard — name ACL

* لاحظ انك كتبت فى الامر الاول (IP & standard) عشان تعرّف ال Router النوع (standard او Extended) لكن فى الارقام فهو بيكونه عارف من الرقم

* الميزه هنا انك بتكتب اسم ال access list مره واحده بس وبعدين بتكتب كل ال IPs مره واحده ، على عكس ال numbered ، كمان لازم تكتب اسم ال access list مع كل IP عايز تعرفه او كل مجموعه IPs مع بعض

* وكمان من ميزة انك لو عايز تمسح سطر هتمسح السطر لوحده على عكس ال Numbered ACL ← لو كتبت (no access-list 7 ----) ← هيمسح ال ACL 7 كلها

عشان تشوف ال (create ACL) بتكتب ال command دى [# sh access-list]

B) activate access control list (ACL)

(config-if) # ip access list-group number or name {in | out}

in ← while receiving (before routing)

out ← while sending (after routing)

عشان تشوفه بتكتب ال command [# sh ip int]

اهم ال shows اللى هتذاكرها

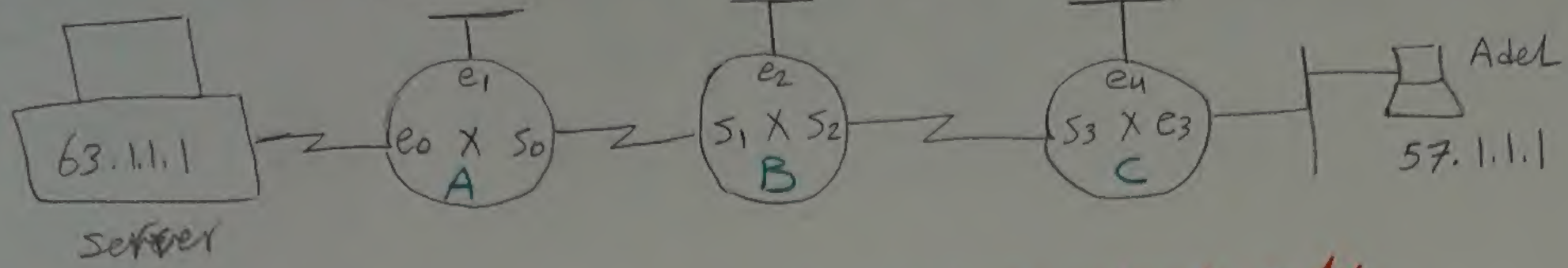
intro : # sh run
sh ip int brief

Routing : # sh ip route
sh ip protocol

Switching : # sh VLAN
sh int trunk

security : # sh access-list
sh ip int

EX



restrict adel only from access to server subnet only

Create

A(config)# ip access-list standard Adel

A(config-std-nacl)# deny 57.1.1.1 [0.0.0.0] ← optian
wcm

A(config-std-nacl)# permit any or 0.0.0.0 255.255.255.255
wild control Mask

activate

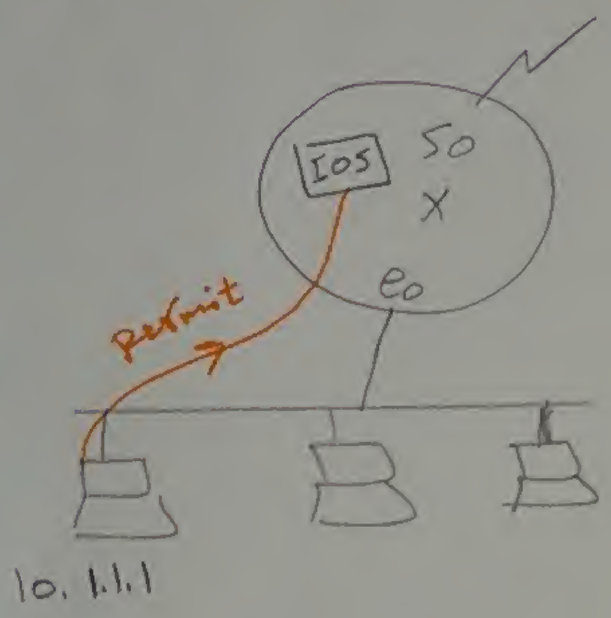
A((config)# int e0

A(config-if)#ip access-group Adel out

← بمعنى ← نفذي الـ ACL اللي اسمه Adel والداتا خارجه من عندك

Rule 1 : access should contain at least 1 permit
Rule 2 : Standard ACL should be placed as close as possible to distination
عشان منخنقش على الـ src

EX



(config)# access-list 3 permit 10.1.1.1

((config)# line VTY 0 4

(config-line)# access-class 3 in → ???

لـ الداخل

② IP Extended ACL

it filters data based on 1- Tcp/IP protocol (L3 & L4 protocol)
2- src IP & dst IP
(option) 3 - application name or port no (L7)

[A] Create ACL

numbered ACL :-

(config)# access-list 100-199 {permit | deny} Tcp/IP protocol src ip w.c.m

dst ip w.c.m [eq Application name | port no]

note

① Tcp/IP protocol → is L3 & L4 protocols as TCP & UDP & ICMP & Eigrp & .....
* If you write (IP), it means any protocol

② W.C.M must be written ⇒ it is not option here but it was option in IP standard ACL

③ [eq Application name | port no] is option, If you don't write it (or)
→ the default will be any

Ex of Application name | port no

FTP	20, 21
SSH	22
Telnet	23
SMTP	25
HTTP	80
HTTPS	443

named ACL :-

(config)# ip access-list extended name

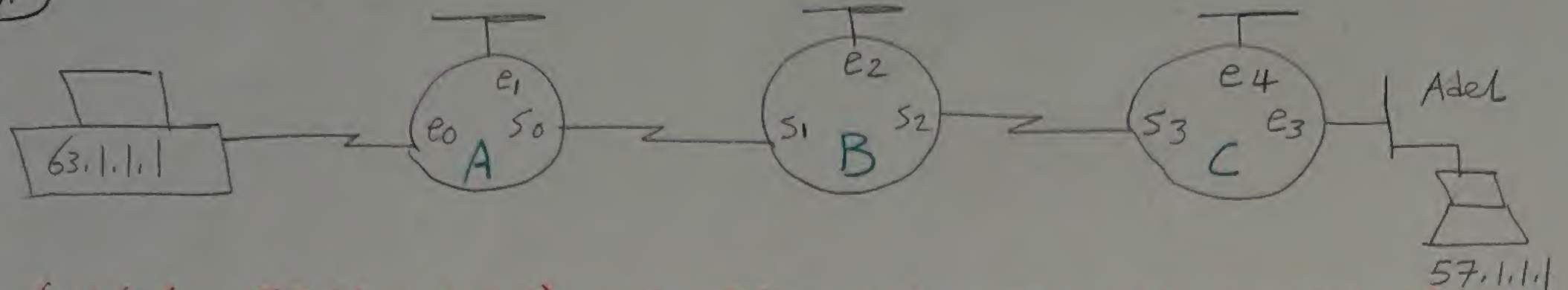
(config-ext-nacl)# {permit | deny} TCP/IP protocol src ip w.c.m

dst ip w.c.m [eq Application name | port no]

[B] Activate ACL :-

(config-if) # ip access-group # or name {in | out}

Ex



Restrict 57.1.1.1 (Adel) only From browsing only on server only

Create (TCP) اللي هو تبع HTTP تبع Browsing عشان لازم

C (config) # access-list 199 deny Tcp 57.1.1.1 0.0.0.0 63.1.1.1 0.0.0.0

eq ~~HTTP~~ WWW

HTTPS & HTTP عشان لازم تكتب

C(config) # access-list 199 permit IP any any

activate

C (config) # int e3

C (config-if) # ip access-group 199 in

Rule 3 : Extended ACL should be placed as close as possible to src

عشان تفلتر ال ip بتاعه صدر الاول خالص عشان ميعملش processing كتير

مع العلم في الحاله دي (Extended) انت اصلا محدد ال dst IP & src IP وبالتالي لو وضعتوها على اي interface (e0, s0, s1, s2, s3, e3) مش هتفرق كتير عشان ميعملش processing كتير

Note / this command (57.1.1.1 src ip 0.0.0.0 wcm) can be shorted to (host 57.1.1.1)

and also (63.1.1.1 dst ip 0.0.0.0 wcm) (host 63.1.1.1)

Security Mitigation (continone)

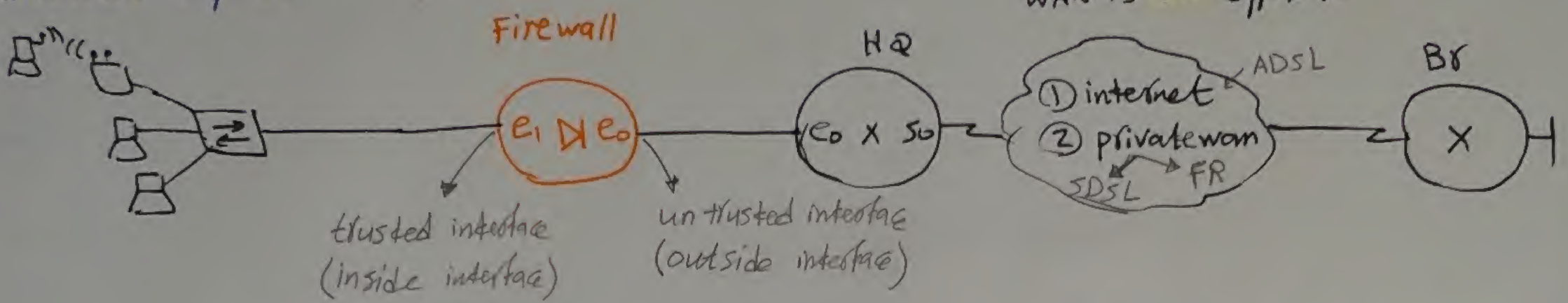
1. switch security
2. Router security

---

3. Firewall ملحوظة / كل ال Interfaces اللى على ال Firewall تبقى Ethernet

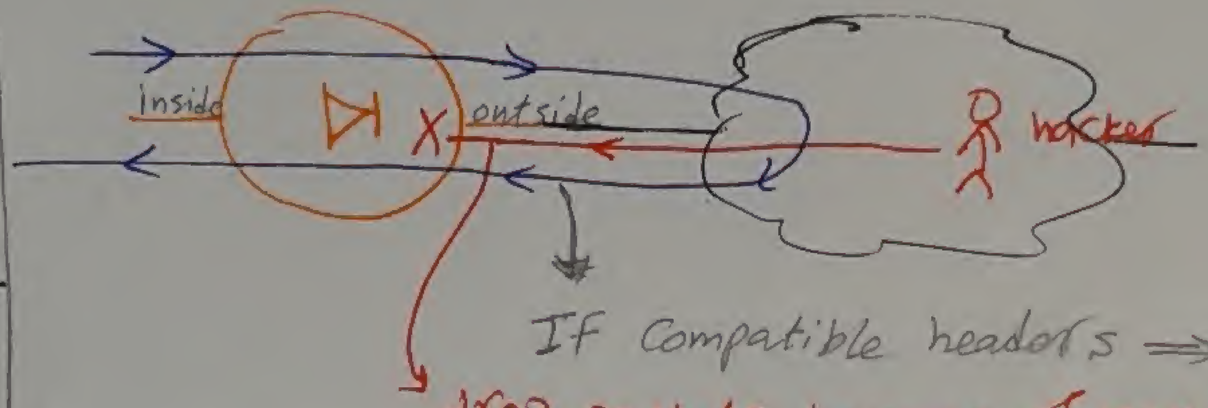
Firewall operation

1. Data From inside allowed to go outside by default
2. Data From outside is not allowed to go inside unless it is a reply For internal request



inspection table

L3 & L4 headers
src ip , dst ip
Tos , TTL
, protocol , src port
, dst port , squ #
, Ack , -----

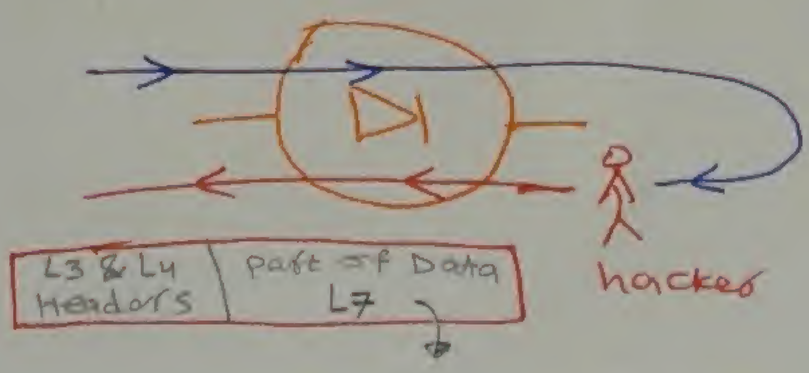


If Compatible headers ⟹ permit to enter
drop packets because of non compatible headers

ال Firewall فيه inspection table اللى موجود فيه (L3&L4 headers) من ال Frames اللى خارجه منه

⟸ اى packet داخله من outside ⟸ ال Firewall بيشوف ال L3&L4 headers و صيكا بقعم بالى عنده فى ال inspection table ٥ لو compatible headers صيسمح لل packet بالدخول فقط

ولكنه موجود bug ٥ وهى انه ال hacker يقدر ياخد اى packet راجعه ويسيب ال headers زى ماهمى بس يغيّر فى ال Data نفسها ويحط Virus فيها



Malicious File
مؤذى

ساعتها ال Firewall صيسمحلها تدخل مادام ال L4&L3 protocols compatible

حل المشكلة دى ⟸ فى انه كمان Cisco

PIX Firewall (Application wirefall)
(deep inspection)
L7 inspection

PIX Firewall

Application Firewall
(deep inspection (L7))

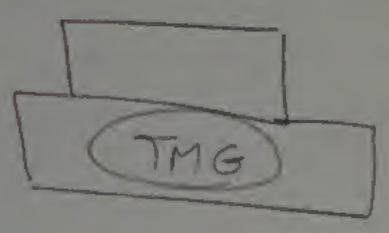
Softwere ↓ — Hardwere ↓

ISA by Microsoft

(بعد التطوير) ← كتير bugs لكن طلع فيه

TMG

(Thread Management Gateway)



هتسطب البرنامج على pc

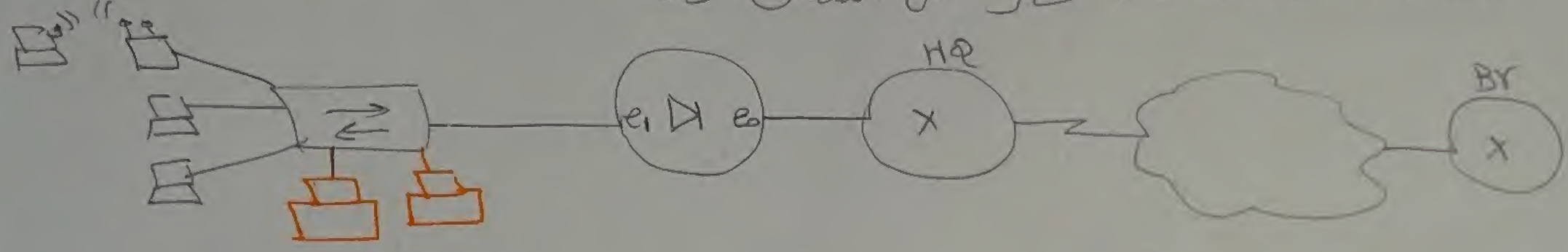
زيها بس فيه انه بطئ اوى عشان الـ S/W

ASA by cisco

(adaptive security Appliance) — H/W

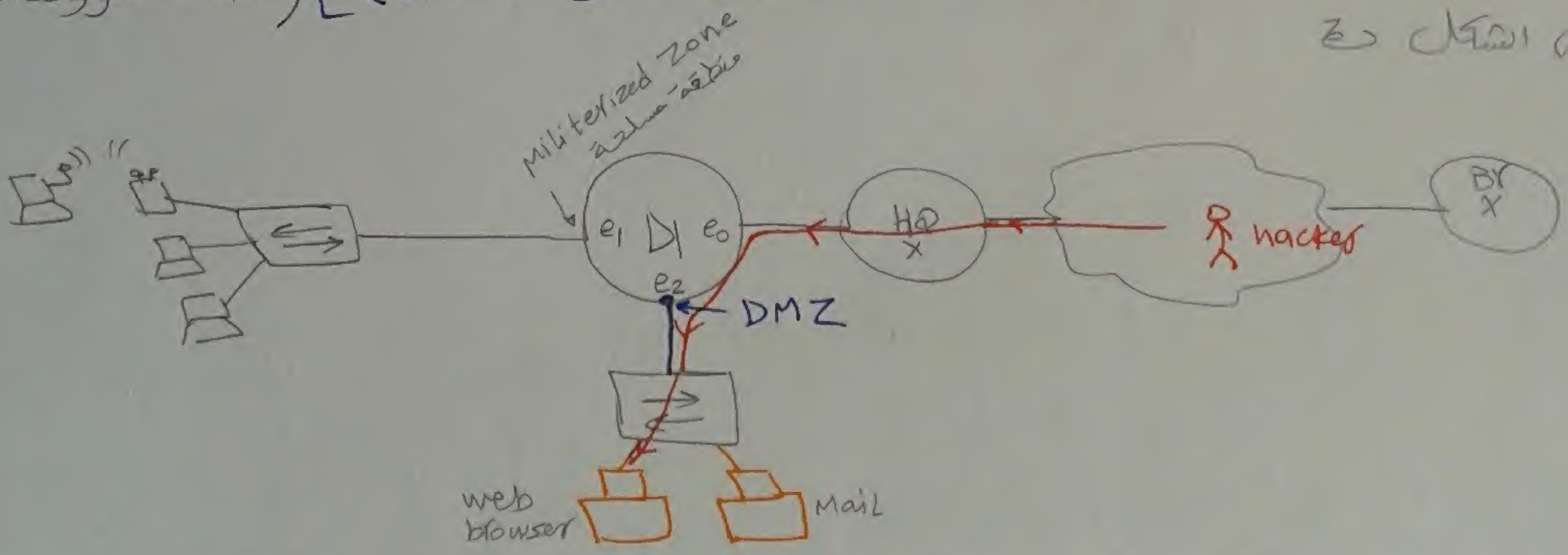
سريع جدا عشانه H/W بس غالى اوى

لو انت عندك servers فى الـ LAN اللى فى الـ HQ وعايز ناس من اللى موجودين فى الـ BR يدخلوا على الـ servers دى ← كده انت هتفتح ثغرة فى الـ Firewall لكده ده خطر فى الشكل دة



الحل للمشكلة دى انك هتشترى Firewall له رجول جديدة غير (inside&outside) والرجول دى اسمها [De-Militerized zone (DMZ)] (منطقة منزوعة السلاح)

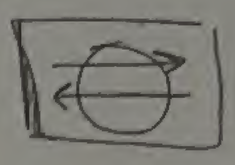
فى الشكل دة



وبالتالى لو الـ Haker عايز يدخل على الـ LAN بتاعتك ← مش هيقدر يعبر من الـ firewall لانه هيعدى عن طريق الـ interface (DMZ)

بكده مازل هناك خطر ← انا بالفعل اقدرت احمي ال LAN من ال haker
بكده ما زال ال servers معرضه للخطر ويقدر ال hacker يدخل يخرّب فيهم
← عشانه كده كانه الحل في IDS

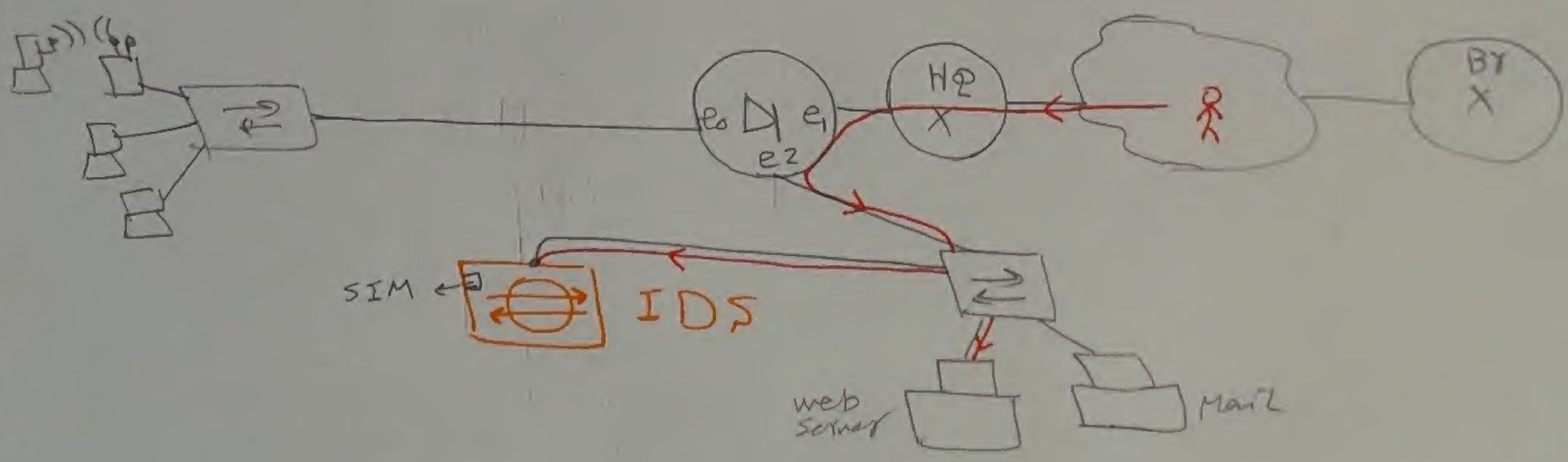
3) IDS (Intrusion Detection system) ⇒ وهزه



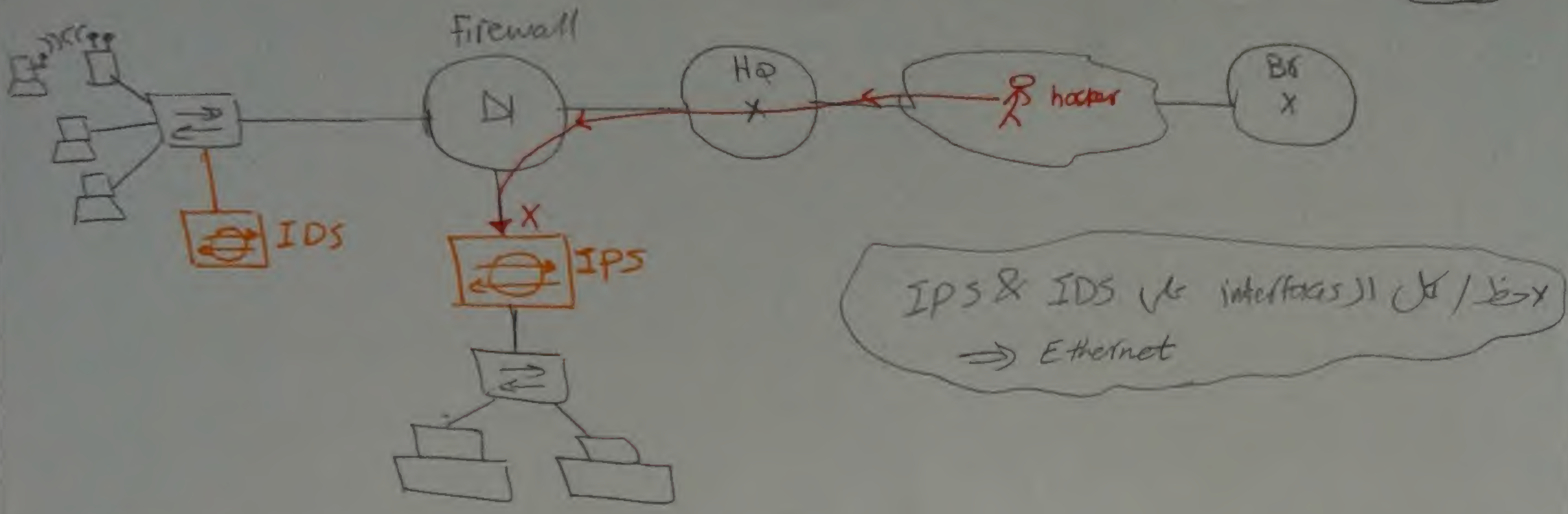
IDS operation

- IDS compares data to attacks signature file
→ If no attack → no response
→ If attack → send alarm to adminstrator

ودة عبارة عن sensor او Detector فقط
كل اللي بيعمله انه عنده File اسمه (attak signature file) ودة بيبقى فيه
كل انواع ال (attakes) اللي تم اختراعها من قبل (all known attacks)
* كل packet بتدخل عليه ← بيدخل على كل ال Data ويقارن ال Data دي بال attacks اللي عنده
← لو ال Data مطلعتش attack هيسمح لها بالدخول
← ~ ← ال Data طلعت attack ← هيرسل alarm او SMS message
لل Mobile بتاع ال Adminstrator وهو يتصرف



لكنهم اخترعوا ال IPS (intrusion prevention sys.) ودة افضل من IDS
عشانه بيقدر يمنع ال attack من الدخول على ال servers اصلاً + انه
بيقوم بنفس عمل ال IDS في انه بيبعت رساله لل admin.
وكمان كانه من الافضل انك استخدم ال IDS داخل ال LAN عشانه اعرف
من خلاله محاولات الاختراق داخل ال LAN و اجهزة الموظفين



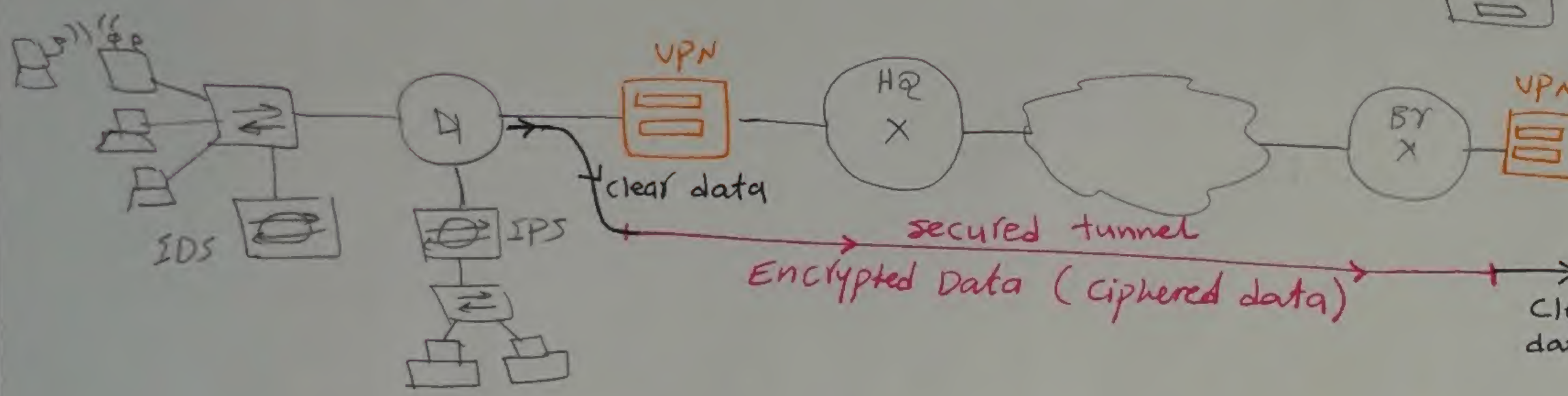
IPS operation

- IPS compares data to attacks signature file

→ If no attack → forword data

→ If attak → stop attak & send alarm to adminstrator

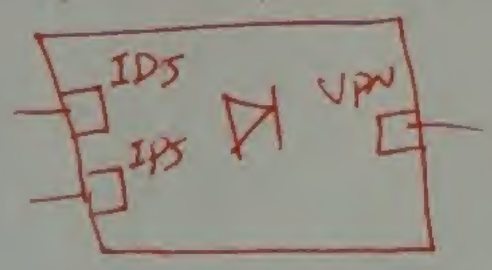
4 VPN appliana : (vertual private network appliana) هو



note

ASA Firewall is made by cisco

it has as buit in all these devices (VPN , IPS , IDS)



ASA firewall

① VPN devices

1. VPN appliance
2. ASA
3. Router

② VPN protocols

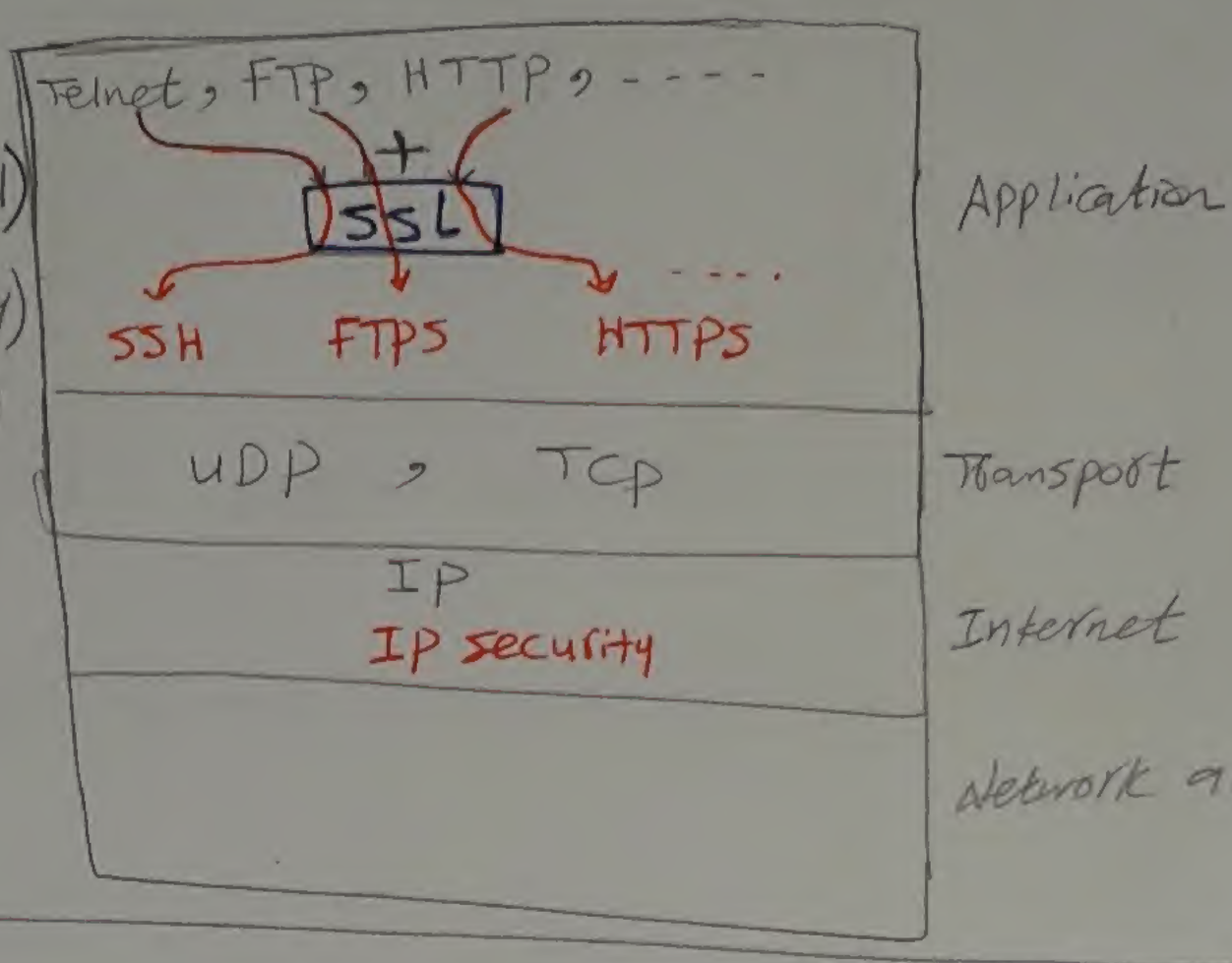
protocols that do confedentiality & Integrety & Authentication

SSL : secure socket layer

Telnet + SSL → SSH (secure shell)

FTP + SSL → FTPS (FTP security)

HTTP + SSL → HTTP (HTTP security)



* IPsecurity is ~~more~~ stronger

③ VPN operation (C, I, A)

Confedentiality
سرية المعلومة
(data Encryption)

→ symetric Encryption key
(Encrpted key = decr. key)

EX1 : DES : Data Encry. Standard
EX2 : 3DES : 3rd ~ ~ ~
EX3 : AES : Advanced Encry. Standard
EX1 اقوى من EX2 اقوى من EX3

→ Asymetric Encryption key
(Enc. key ≠ decry. key)

EX1 : RSA : rivest shmir adel man
EX2 : ELGAmal

EX1 اقوى من EX2

Integrity
سلامة المعلومة
(data Hashing)
(digital signature)

HMAC -MD5 (128 bit)
HMAC -SHA (156 bit)

HMAC : (Hash Based Message Authentication Code)

كل packet مبعت مع 128 bit كأضافة

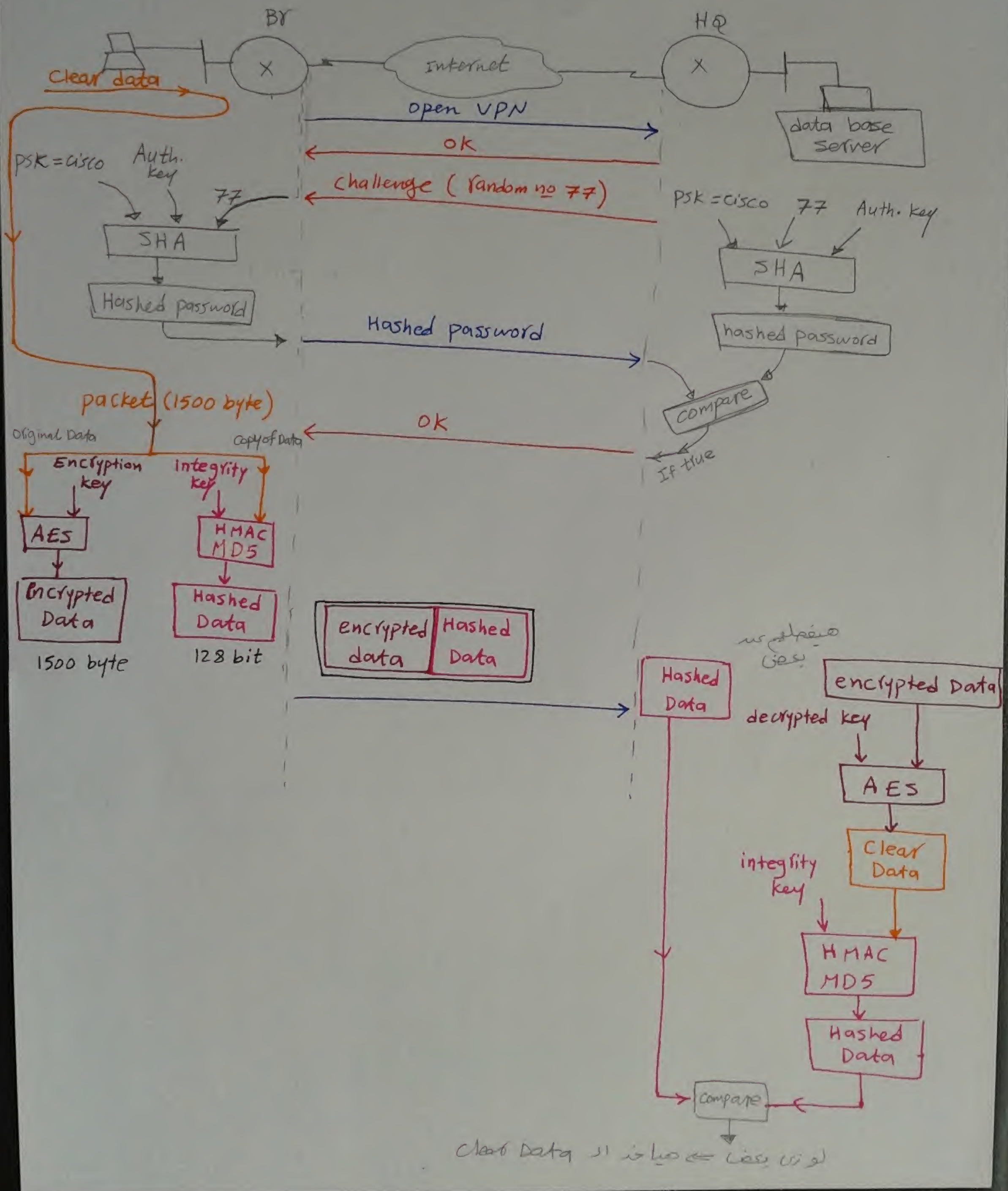
Authentication
التأكد من مصدر المعلومة
(password hashing)

MD5
(Message digester V.5)
50 day بتاعة بعد pass يكسر ال
برامج التشويه الاعتماد
ال hacker يقدر يكسر ال password
50 month بتاعة بعد
(قوى جدا)

→ SHA
(secure Hashed algorithm)

note/ PSK is (pre-shared key), it is a password that ~~is~~ well-known
In both server in HQ and PC in BR

العملية دى بطيئة جدا لكنها جعلت الـ security فى منتهى القوة

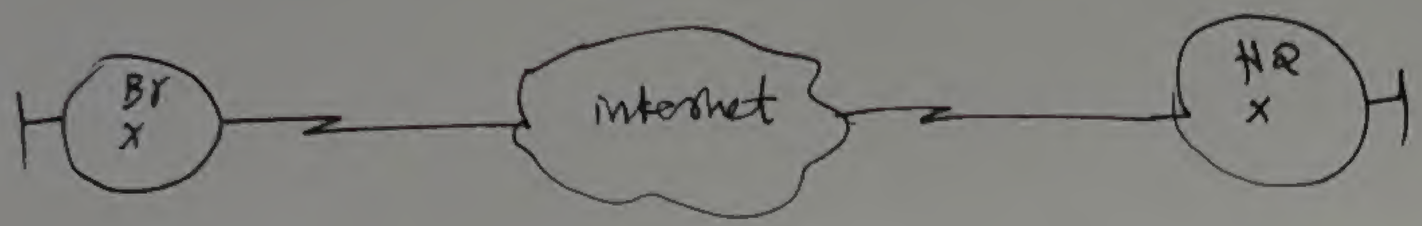


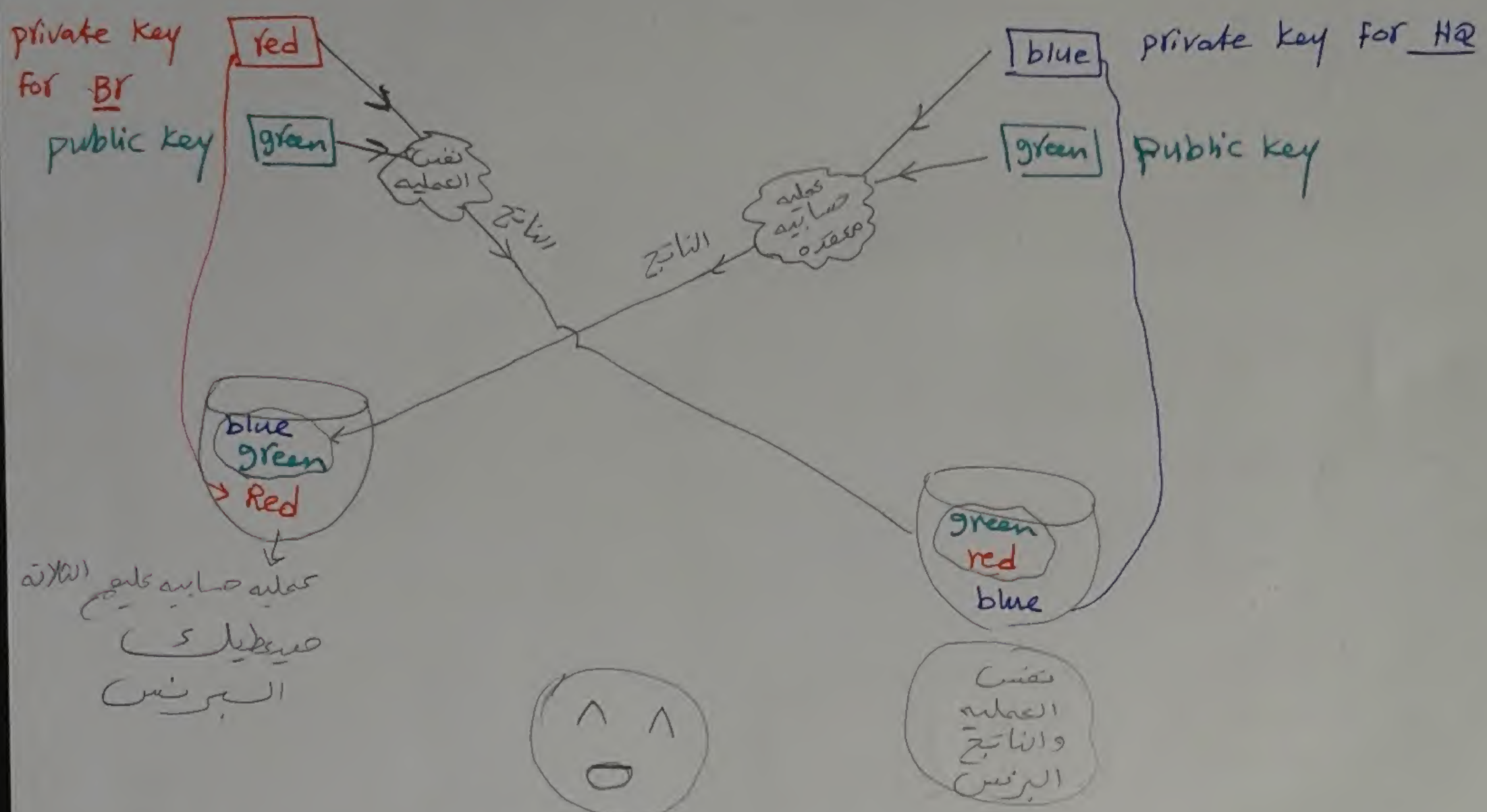
ناقص اخر حاجه وهو انى اعرف ازاى يكوّن الـ Keys الـ Encryption & Auth. & integrity

⇐ من الواقع البزنس = Encryption key = Authintication key = integrity key

IKE [internet key Exchange)

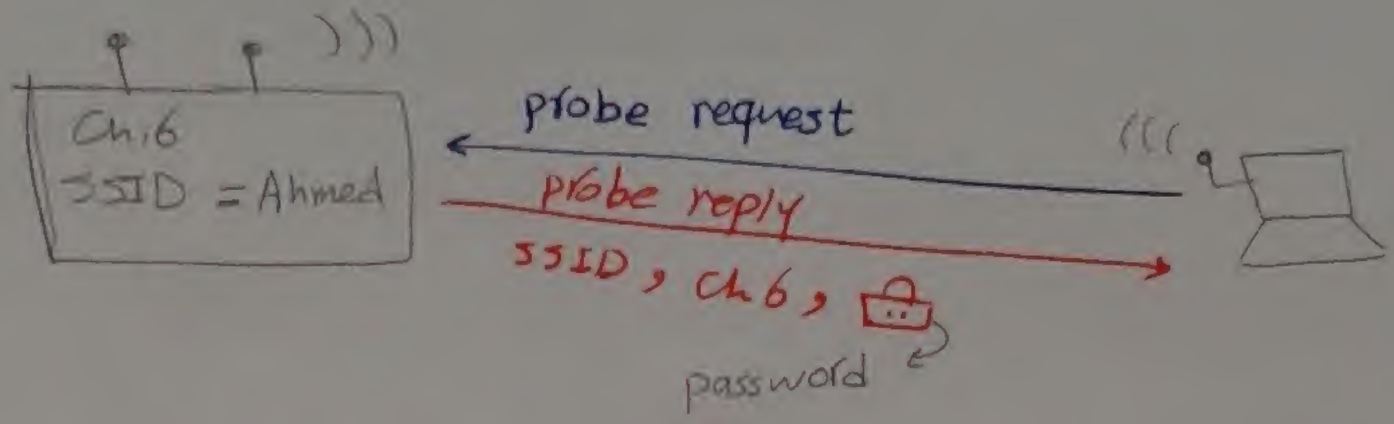
by Diffie - Hellman





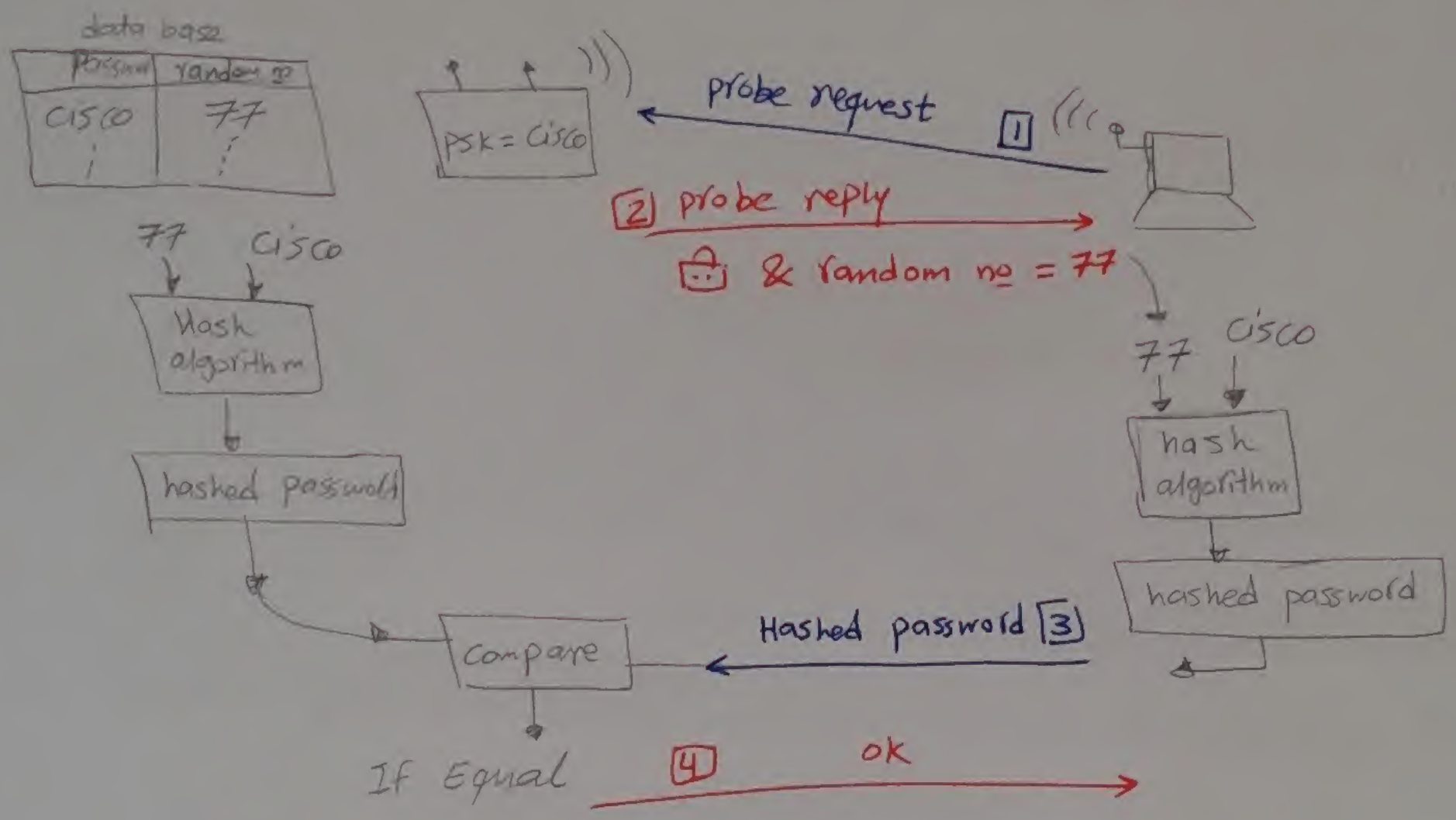
البزنس ده By default بيتغير كل 8 hr وممكن تغييره بالـ Configuration الى 4 hr

wifi security



Security types :-

[1] PSK (pre-shared key)

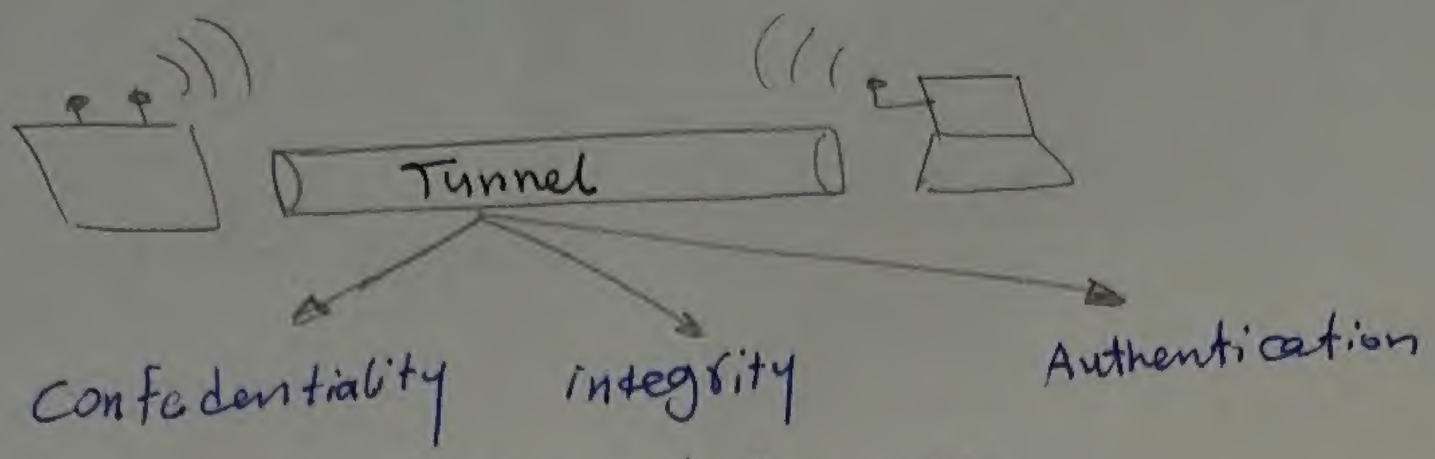


* عيب النوع ده انه اضرب صد زائد (weak algorithm)
* اسم الكراك اللى قصر يحل ال algorithm ده

air crack ≡ psk crack ≡ WEP crack

WEP = wire less equipment protocol

[2] w PA (wifi protected access)

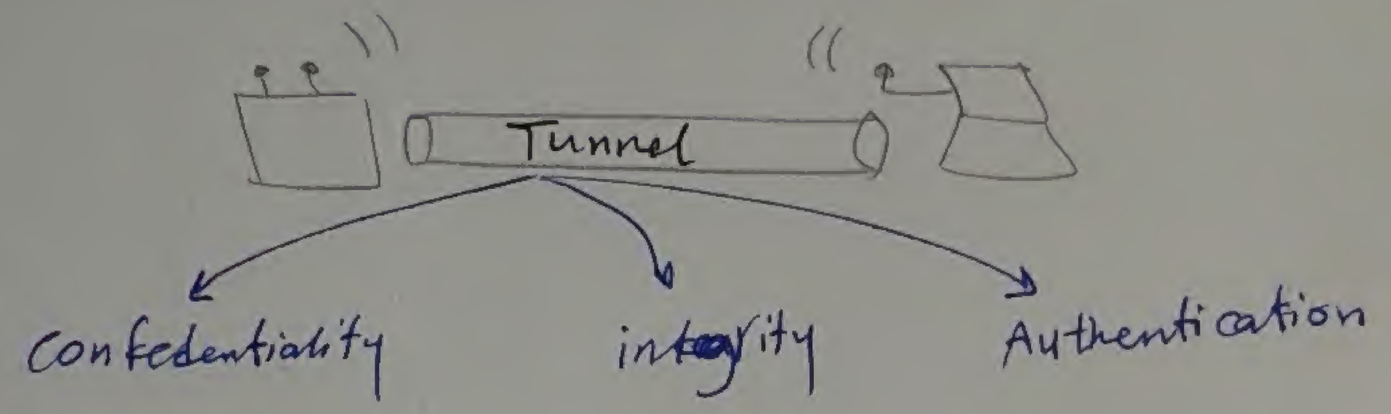


the programs & protocols that used in WAP

① MIC [Message integrity code] is used for integrity process
② TkIp [Temporary key integrity protocol] for confedentiality & Authentication

كنت للاسف اتضرب لكنه خد وقت كبير بقبال ما حلوا ال pass بتاعته

[3] wPA 2 ← الاقوى و متضربش لحد دلوقتى



it is using strong algorithm who is :-

① AES (advanced Encryption Standard), but still use TKIP to backward compatibility with WPA

IPV6

IPV6 is the next Generation Network (NGN)

* تم تطبيقه فى مصر 6/2012

Why we need IPV6 ?

we need larger address space

① internet population is increasing

② mobile phones, PC, Notepad, -----

③ Transportation

④ home appliances [smart house]

IPV6 : 128 bit

no of IPs address = $2^{128} \simeq 3.4 * 10^{38}$ IPV6

$\simeq 5 * 10^{28}$ IPV6/human

Colon ≡ :

* IPV6 is 128 bit represented in Coloned Hexadecimal

note IPV4 is dotted decimal ⟹ 4 octets [one octet = 8 bit]

* IPV6 is 8 Fields ∴ IPV6 = 8 * 16 = 128 bit

→ each Field is (16 bit ≡ 4 hexadecimal)

(ex1) 203B : 0007 : 00A4 : 0BDF : 0000 : 0000 : 0000 : 0ACD

* IPV6 address rules :-

[1] leading zeros are optional in a feild

203B : 7 : A4 : BDF : 0 : 0 : 0 : ACD

[2] Field of all zeroes = :0:

203B : 7 : A4 : BDF : 0 : 0 : 0 : ACD

[3] fields of successive zeroes = :: ← it is used only once in IPV6

203B : 7 : A4 : BDF :: ACD ← يمكن ان كل اللى فى النص اصفار

(ex2) 203B : 0000 : 0000 : ABCD : 0000 : 0000 : 0000 : 1234

203B :: ABCD :: 1234 → ✗ يمكن (::) مرتين فى نفس الـ IPV6 عشان الـ pc مش هيفهم كام صفر عند الاولى و كام عند الثانيه

✓ 203B :: ABCD : 0 : 0 : 0 : 1234 او ✓ 203B : 0 : 0 : ABCD :: 1234

(EX3) FF02 :0:0:0:0:0:0:0005

⇓

FF02 :: 5 ⟶ (المناظر له في IPV4) 224.0.0.5

all OSPF3 routers → OSPF2 with IPV6

all OSPF2 routers

* ال OSPF اللي اتعلمناه في ال Routing اسمه (OSPF2)

(EX4) 0:0:0:0:0:0:0:1

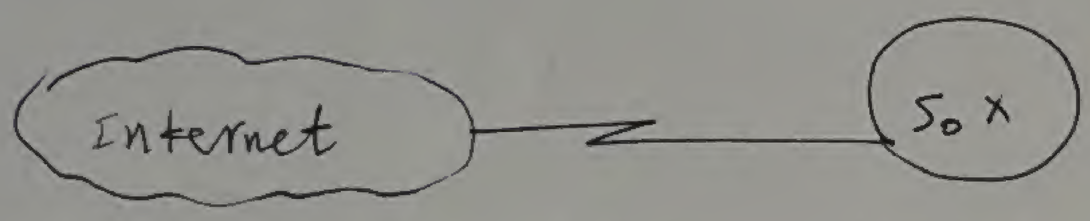
⇓

::1 ⟶ (المناظر له في IPV4) 127.0.0.1

all IPV6 loopback Icp/IP

loopback ⟹ TCP/IP

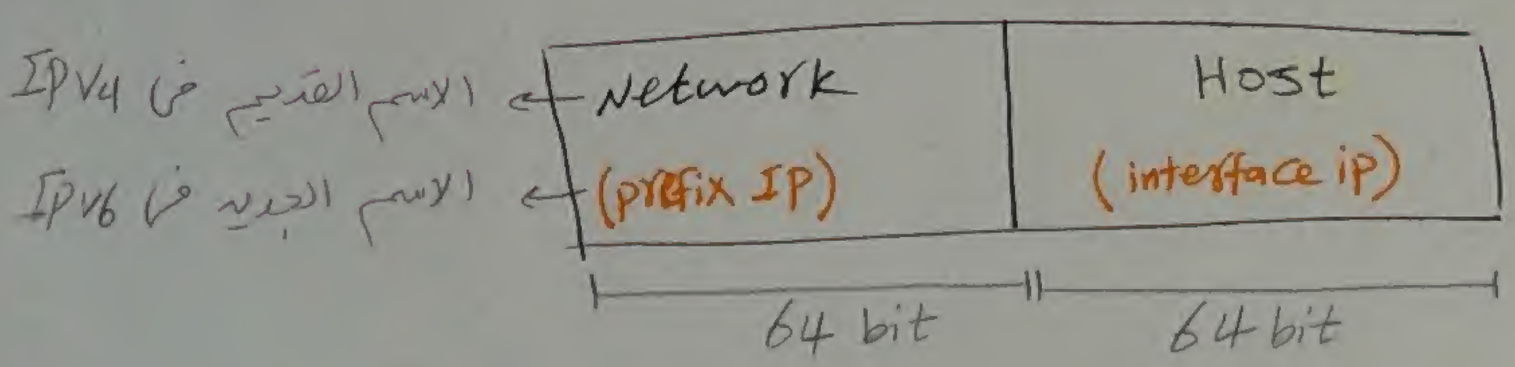
(EX5)



(config) # ip route 0.0.0.0 0.0.0.0 S0 ⇐ in IPV4

(config) # ipv6 route :: 10 S0 ⇐ in IPV6

IPV6 class is called default class ⇐ there is only one class in IPV6



The default mask /64

How to give IP to DTE ???

1. Statically
2. Dynamically by using DHCPV6
3. Dynamically by using NDP [Neighbor discovery protocol]

---

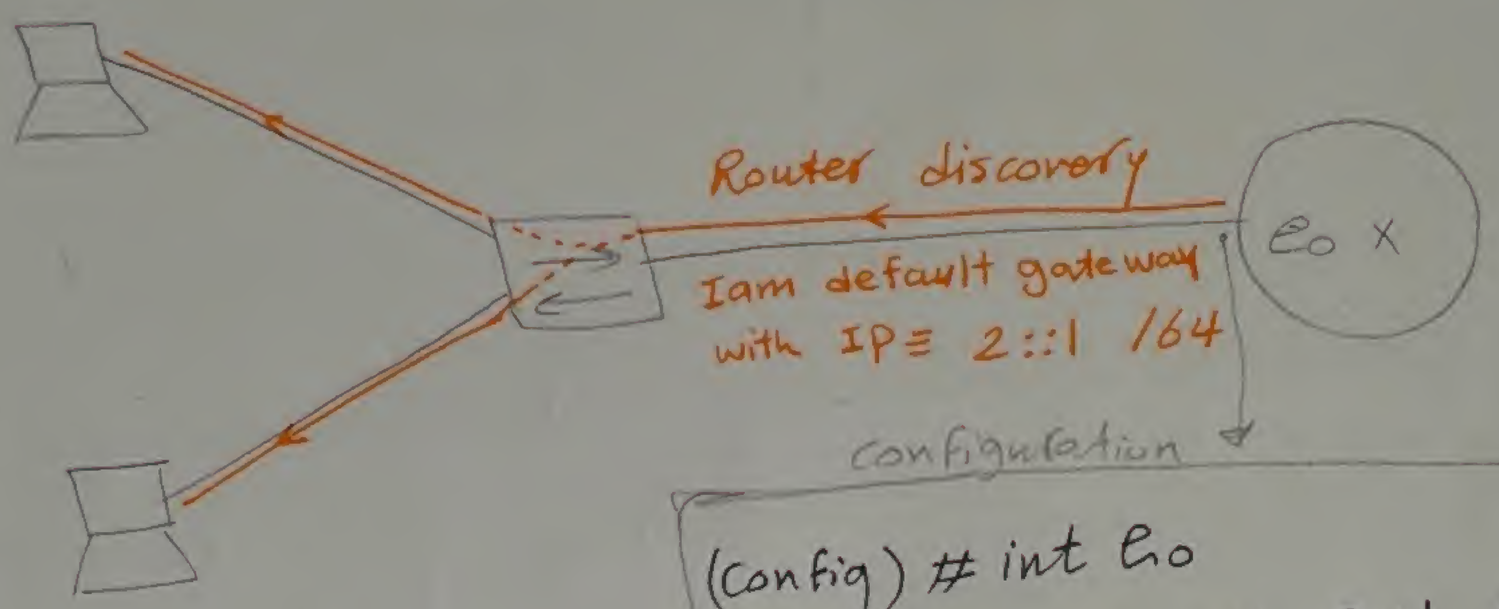
* NDP operation

network / host part

IP: 2:0:0:0: - - - - - -
mask: /64
d.g: 2::1

network / host part

IP: 2:0:0:0: - - - - - -
mask: /64
d.g: 2::1




```
(config) # int Eo
(config-if) # ipv6 add 2::1 /64
```

2::1 /64

2:0:0:0:0:0:0:1

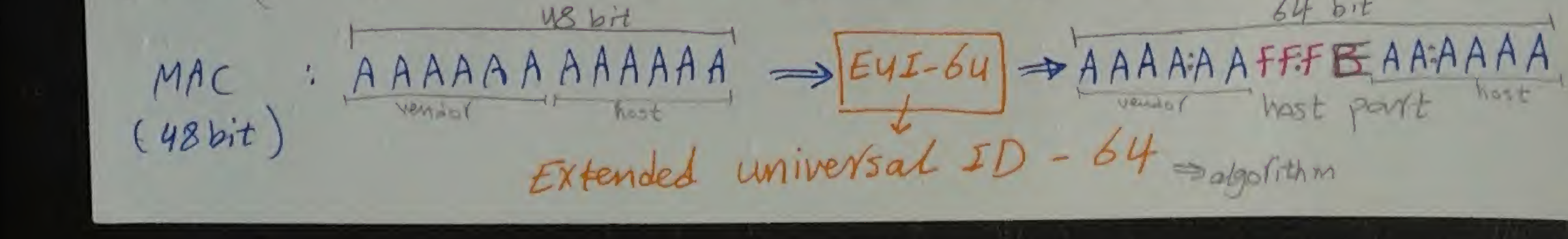
N H

(FF02::2)
Broad cast الروتر بالامرين اللي فوق ده هيبعت على ال

* بعد ما ت configure
ال (Router discovery) وهيقول فيه [انا ال d.g و ال Ip & Mask 2::1 /64]

* كل pc هياخد ال (Network part) من ال Ip وهيضيفه لنفسه وهياخد ال MAC address بتاعه (48 bit) وهيدخله على protocol اسمه (EUI-64) عشان يضيف 12 bit زيادة لل MAC ويبقى الناتج 64bit ⇐ ال pc هياخد ال 64 bit دول وهيجعلهم ال host part بتاعه

* ملحوظة ال 12 bit الزيادة هما (FFFE Hexa) ودول ثابتين ومكانهم كدا



IPV4 types

unicast
Class A
Class B
Class C

Multicast
Class D
224.x.x.x
239.x.x.x

all Routers multicast → 224.0.0.2
all OSPF2 → 224.0.0.5
DR & BDR OSPF2 → 224.0.0.6
RIP V2 → 224.0.0.9
EIGRP → 224.0.0.10

Broadcast
255.255.255.255
it is used for protocols as (RIPV1, EIGRP) and application as (DHCP)

IPV6 types

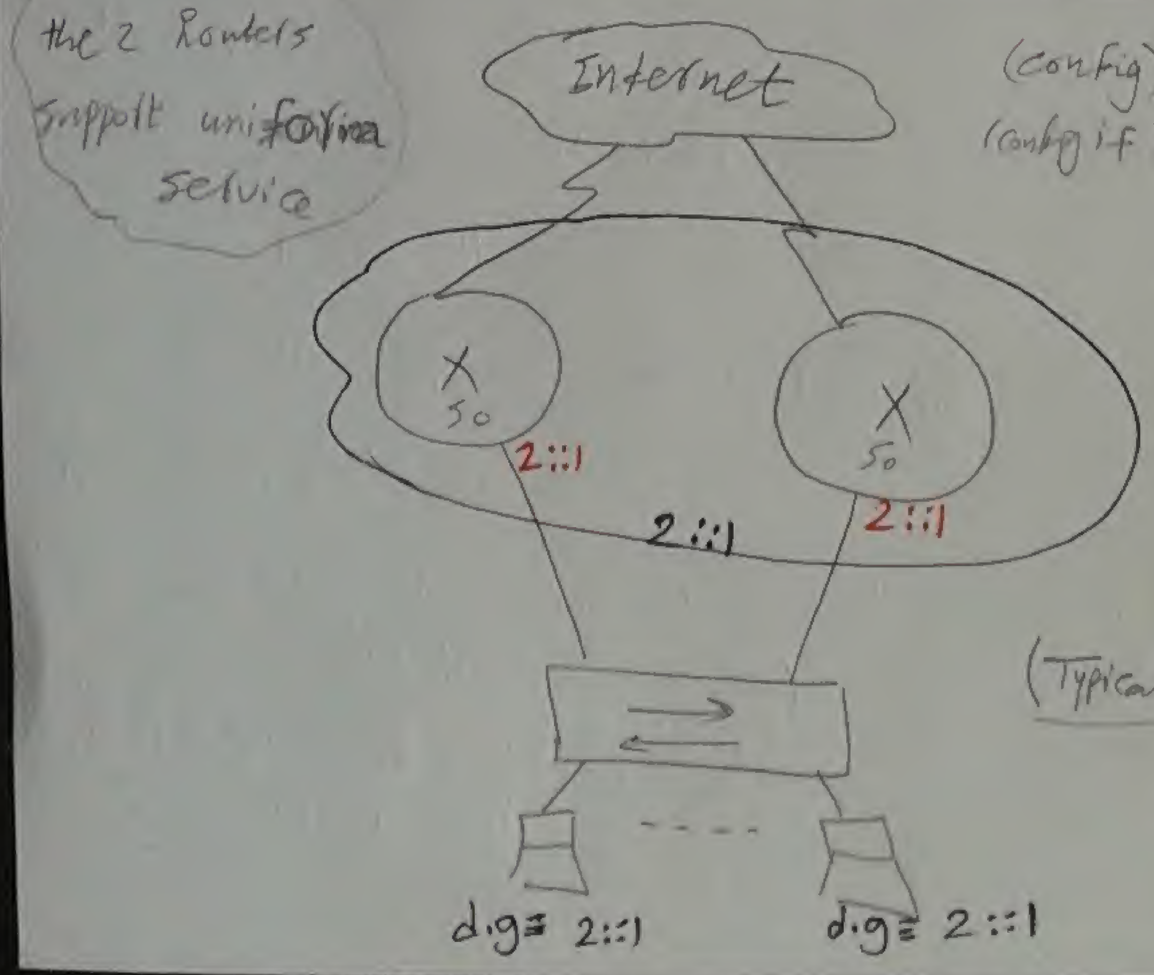
unicast

Multicast
Network | Host
FFxx : ——

all IPV6 Routers ← FF02::2
OSPF V3 ← FF02::5, FF02::6
RIP ng (next generation) ← FF02::9
EIGRP for IPV6 ← FF02::A

Broadcast
not supported
في IPV6 مفيش حاجة اسمها Broadcast خالص بيشتغل كل الاجهزة في الشبكة وبيشتغل اي حاجة كانت بتشتغل Broadcast (بيخليها) Multicast
FF02::2 دي الـ IP بتاعت الـ DHCP يعني هلاقي الـ DHCP هيشتغل على الـ Multicast IP بتاعت FF02::2

anycast
- الموضوع هنا عشان ازود الـ Redundancy & loadsharing
مستخدم 2 Routers متوصلين parallel يعني بنفس الـ LAN من طرف وبنفس الـ WAN من الطرف التاني
يعني
more than one router acts as one big virtual router and give them one big virtual IP
(ليهم نفس الـ IP)
العملية دي بيسموها ← uniform service
(Typical يعني) لازم يكونوا الروترين
من انواع الـ protocols اللي بتعمل العملية دي
1- HSRP
2- VRRP ← اتكلم عنهم



(config)# int S0
(config if)# IPv6 add 2::1 /64 anycast

IPV4 unicast

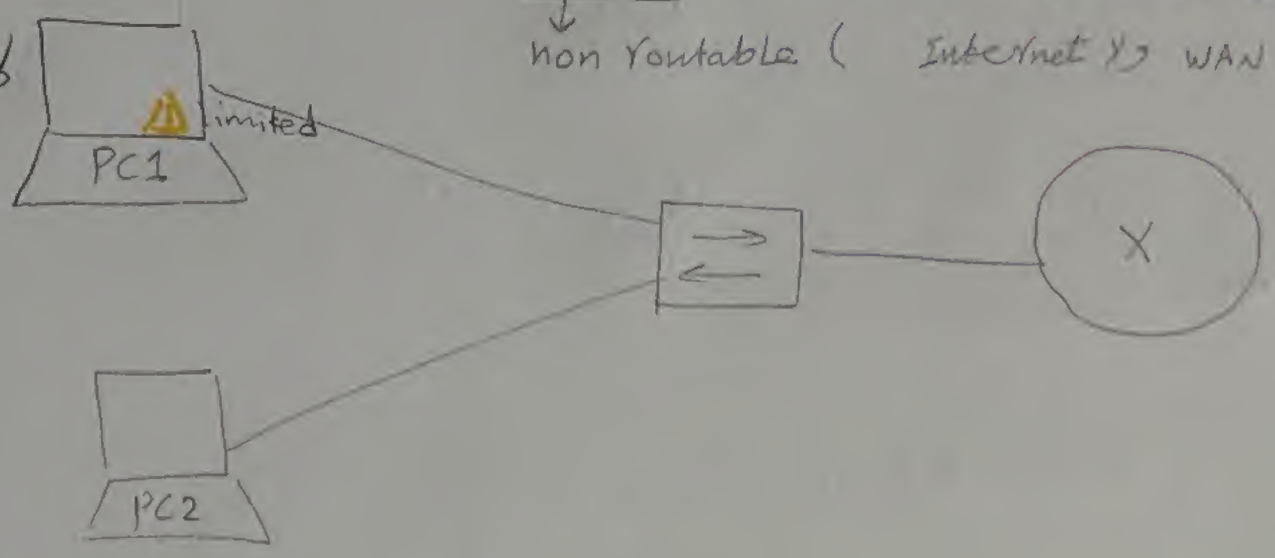
- **loopback**
  - 127.0.0.1
  - مشان تكلم بيها نفسك
  - TCP/IP عال ping ← بتاعك
- **private IP in LAN**
  - مشان تكلم بيه اي حد من ال LAN بتاعتك بس
  - (EX) - manually
    - Automaicaly
      - DHCP
      - APIPA
- **private IP in LAN / WAN**
  - 10.x.x.x
  - 192.168.x.x
  - 172.16.x.x → 172.31.x.x
- **Real IP (public IP)**

IPV6 unicast

- **loopback**
  - ::1
- **Link local**
  - FE80 : x
  - (EX) APIPA
- **Site local**
  - FEC0 (zero) : x
- **global**
  - (public IP)
  - لو طالع بت فقط

- Omanually
- O Automatically → DHCP
  - → APIPA (Automatic private IP address)
    - non routable (Internet في WAN حاجه)

169.254.x.x/16



لو انت شغال (DHCP) وفي مشكله معينة في الDHCP server والـ PC1 مش عارف يأخد IP من الـ DHCP server ← اولاً هتظهر علامه صفراء في الـ PC وهيقولك فيه limited access

← هنا لازم الـ PC1 ياخد اي IP عشان يشتغل فهيروح واخد اي IP من الرينج ده 169.254.x.x /16 لازم نتأكد الاول انه مفيش حد واخد الـ IP ده قبل كده

الـ protocol اللي بينفذ العملية دي اسمه APIPA

* IPV6 end to end data delivery

يوجد 7 تحسينات اضافية IPV4 عن IPV6

[1] Enhancing blug & play configuration (NDP & EUI-64)

[2] Enhancing redandancy & loadsharing (any cast)

[3] same routing protocol (RIP ng , ospf3 , static , EIGRP , ----)

[4] Enhancing Integrated QOS (Buit in header COS)

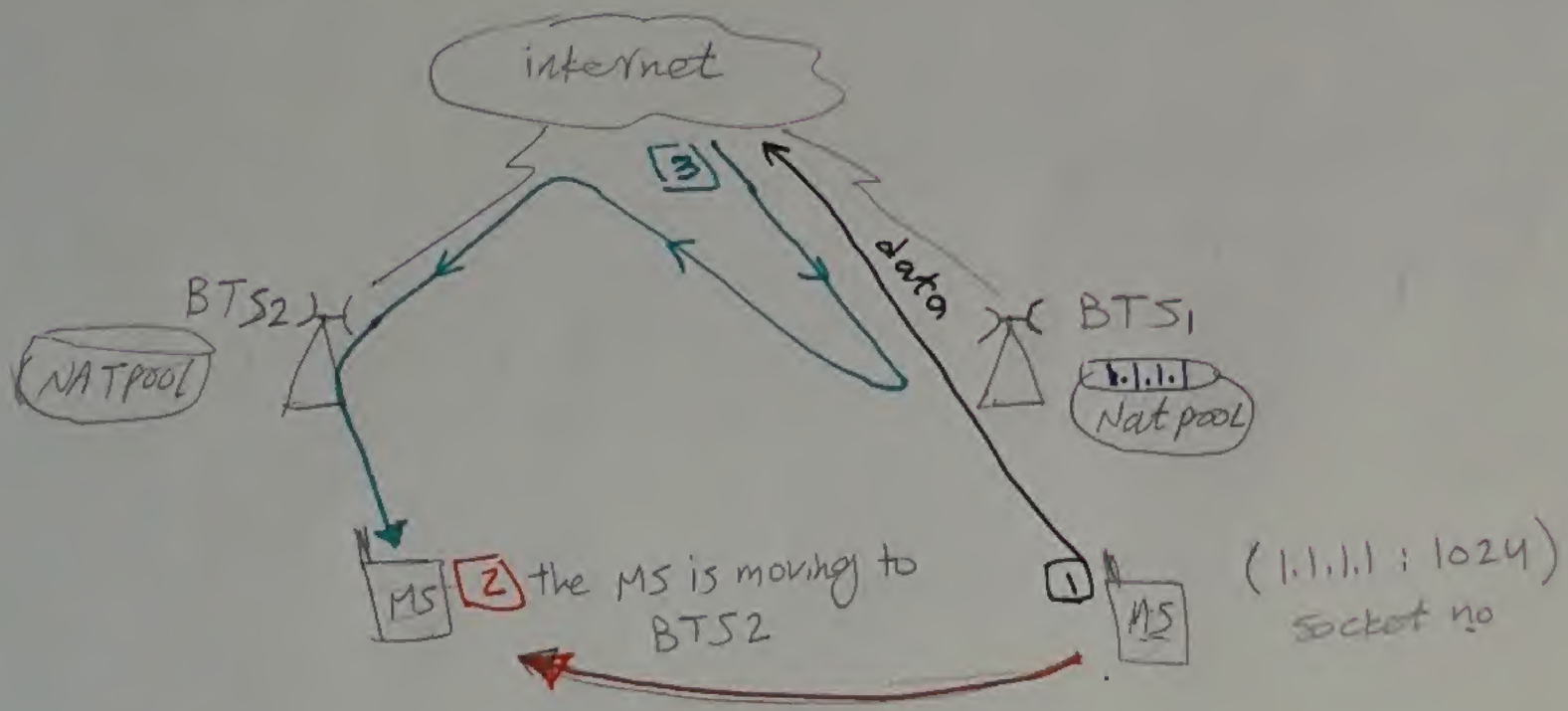
class of service ⇒ 8 bit for periority

[5] Enhancing integrated security (Built in header IPsec)

يعني بيتم فيه ⇐ Confedintiality integrity authentica

بدي اعمل VPN

[6] Enhancing Mobility (protocol in header Mobile IP)



لو انت معاك MS وفاتح session جاية في الـ Facebook و "Yahoo" socket no

(Ip : port) ⇐ لو انت بتتحرك بالـ MS من BTS1 الى BTS2 ⇐ لو الـ IP اتغير ⇐ الـ Data متقطع مافهاش مشكلة تغير الـ socket no بتاعك خالص طول ما انت فاتح الـ session و بالتالي كلما هتتحرك من BTS1 الى BTS2 و BTS1 هتقول لـ BTS2 تلغي الـ IP (1.1.1.1) عندك

⇐ الكلام ده بيتم من طريق Mobile Ip protocol

7 Enhancing integerated advanced switching (Buit in header MPLS)
(label switching)

MPLS : Multiprotocol label switching

المشكله / ان شركات الـ service provider لو جت packet IP جين ع الروتر هيقارن الـ IP ده بالـ Routing table اللى عنده عشانه يـ Route الـ packet
بكره المشكلة هنا انه بعض الـ Routing table بيكون فيه حوالى 300,000 ف
وكل الشغل ده من الروتر بيكون S/W ⇐ عشانه كده العملية دى بتخنق الروترات
اوى وكمان كل ما هتضيف new Technolgy هتخنق الروترات اكتر
⇐ العملية دى بطيئه جداً عشانه كده الناس فكرت انها تستخدم الـ (label switching) يعنى هتعمل جدول مناظر الـ Routing table بس مفهوش اى تفاصيل [Mask, protocol] مجرد علاقة لكل Ip موجود فى الـ Routing table
واول ما الـ packet هييجى، هتروح الـ lable switching وهو مش عيرف هيروح فين اى تفاصيل (يعنى بالـ label بس) هيروح الـ Next hop router
اللى بينفذ الـ lable switching عبارة عن IC (hardware) وده سريع جداً
وبالتالى انا زودت السرعه لـ 10 اضعاف على الاقل
اللى بيقوم بالعمليه دى كلها MPLS

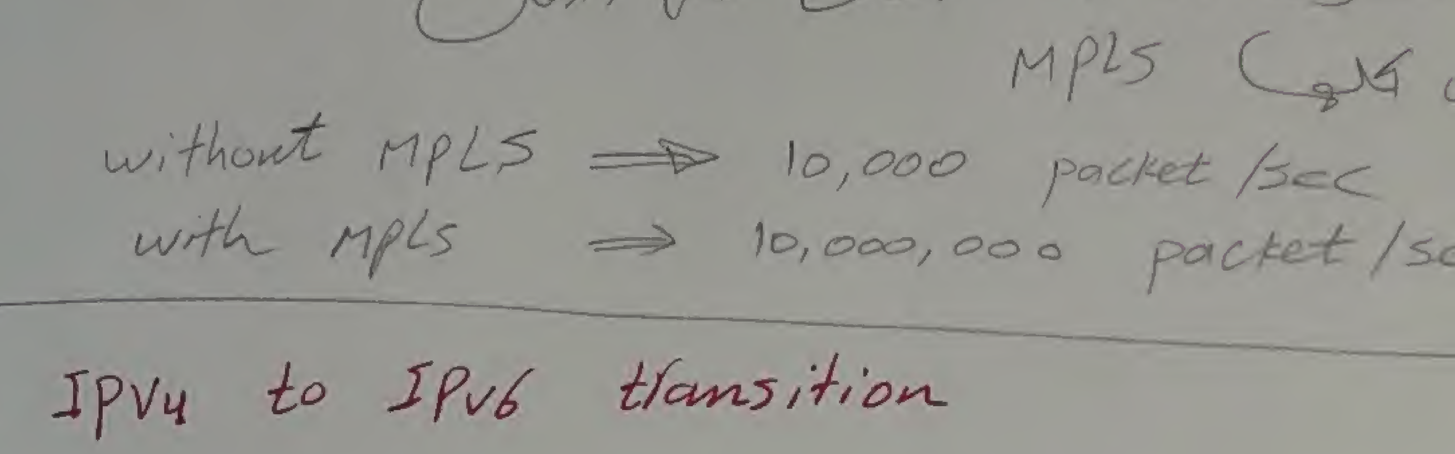
without MPLS ⟹ 10,000 packet/sec
with MPLS ⟹ 10,000,000 packet/sec

---

* IPV4 to IPV6 transition

1 DUAL Stack ⟷ TCP/IP, TCP/IPV6 — OS (operating system) & TCP/IP على الـ TCP/IPV6

2 NAT-PT (NAT protocol Translation)

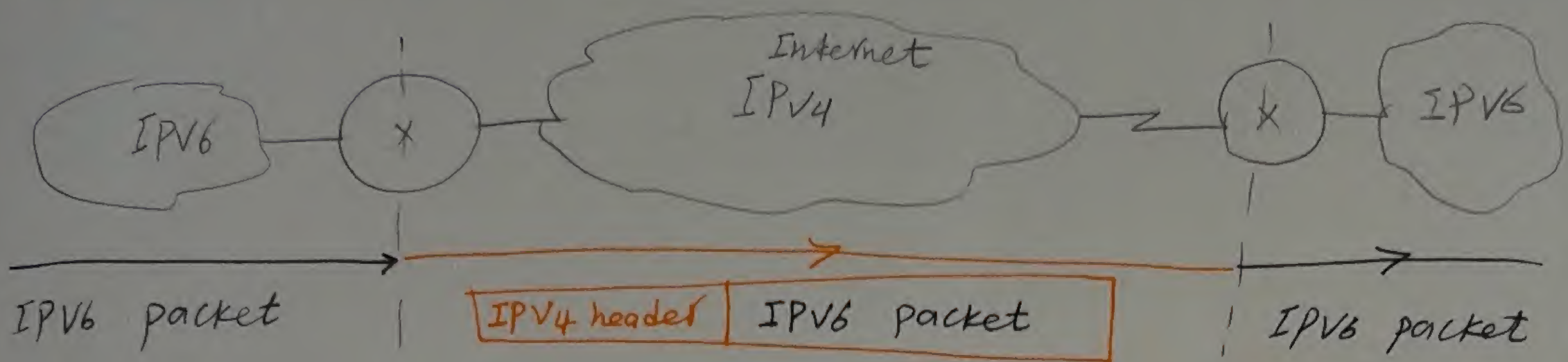


الروتر بيغير شكل الـ headers من IPV4 الى IPV6 ⇐ العمليه دى بطيئة
ومعقدة شويه

DNS server

IPV6	IPV4
=	=

3 Tunneling شغل



IPV4 فيه header الروتر هيضيف
(address ---)

How to Recover password

Router bootup sequance ↗ load IOS
↘ load configuration file

[1] Consult Configuration register

16 bit

By default ⇐ 0X2102 عبارة عن 16 bit (hardwere) IC
↓
Hexa يعني

وشغلتها انها بتستشير الروتر ازى تشغل الـ IOS & Configuration

0X2102
العنوان ده معناه
↙ load IOS normally
↘ load configiration File normally

[2] load IOS normally

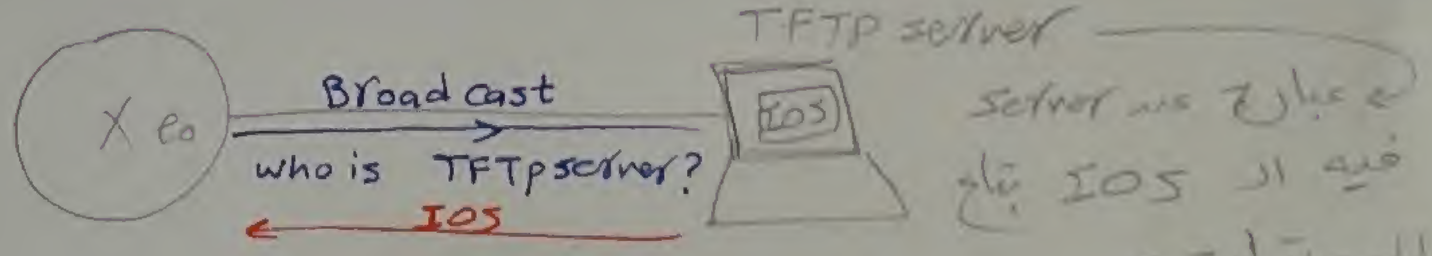
اول ما الروتر بيشتغل بيكون عايز يـ load الـ IOS

فاول حاجه انه صيروح يـ load من الـ flash

ⓐ Flash
ⓑ TFTb
ⓒ Rommon

(الـ flash دى هى الـ Harddisc بتاع الروتر)

لو ملقاش الـ IOS فى الـ Flash ← الروتر هيبعت رساله
على الـ Broadcast يقول فيها مين TFTP server
عشان عايز الـ IOS



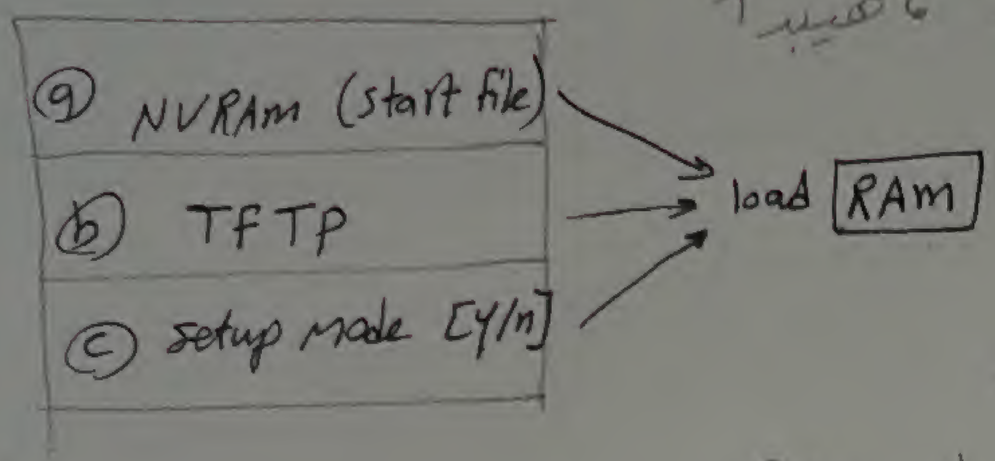
server عبارة عن
فيه الـ IOS بتاع
الروترات

واخر حاجه لو الروتر ملقاش اى TFTp server رد كليه، صيروح يسأل Rommon
والـ Rommon ده عبارة عن (mini operating sytem)

خلّى بالك من الترتيب عشانه بييجى فى الامتحانه
1- Flash
2- TFTP
3- Rommon

[3] load configuration file (ده فيه ال password اللي عايز اكسرها)

بعد ما الروتر هيد ال IOS وهيبدأ



يدور على ال configuration file

اول حاجه هيدور فيها هي ال NVRAm

← لو لقى ال config. file في ال NVRAm هيروح يـ load ال config. file في ال RAM

← لو ملقاش ال config file في ال NVRAm هيروح يدور في ال TFTP

ولو ملقاش هيروح يدور في ال setup mode

password recovery

① power off/on

② press Ctrl /Break (Ctrl/ Break) بسرعة اضغط على ال Flash وال NVRAm ال config. file و ال IOS تحميل ال الروتر هيكملش

← بعد ما تكتب (Ctrl/ Break) هتلاقي نفسك في ال Rommon

③ Rommon > confreg 0x2143

الرقم ده معناه

load IOS normaly

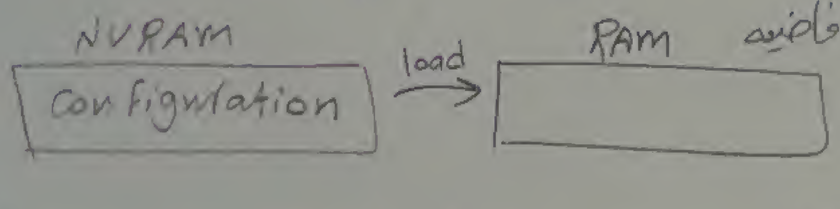
bypass NVRAm (بمعنى مبتبصش على ال password)

④ router Load by passing NVRAM

آه انت هتدخل على ال config وهتساوي

(config) # no enable secret ← تلغي ال passs

(config) # no enable password



آه انت دولقتي عايز تعمل ال config من NVRAm الى ال RAM بالاوامر دة

(config) # copy start run

بعد كده ترجع كل حاجه زي ما كانت عشان ترجع ال config تاني لل NVRAm

config-register 0x2102

sh version